Washington State Fusion Center
INFOCUS
THURSDAY - 5 JAN 2023

	International	National	Regional and Local
Events, Opportunities Go to articles	01/05 Day 316 of the Russia invasion 01/05 Ukraine pleads for tanks from allies 01/05 Ukraine: Russia troops' sexual war crimes 01/05 Students in Iran rise up against government 01/05 NKorea drone near Seoul presidential office 01/04 Ukraine: Russia suffers heavy losses 01/04 For Russia troops: cellphone use lethal 01/04 Ukraine postal workers lead reintegration 01/04 Covid surges in Beijing 01/04 China's unfolding tragedy 01/04 China throttled anti-Covid protests 01/04 WHO worried about China Covid surge 01/04 Australia to deploy US HIMARS 01/04 Russia hypersonic missile-armed ship 01/04 SKorea stands up offensive drone unit 01/04 Iran lashes at France over new cartoons 01/04 Oil falls; mounting global economic worry	01/05 New XBB.1.5 variant 'spreading like wildfire' 01/05 California's 'Pineapple Express' storm 01/04 Mask mandates return to NJ schools 01/04 More job cuts in latest tech worker purge 01/04 Manufacturing weakens on easing demand 01/04 Power grids under assault 01/04 LAPD secretive private funding arm 01/04 Pentagon to bolster Guam's defenses 01/04 Cuban migrants overwhelm Florida Keys 01/04 Auto sales drop to worst level in decade 01/04 More toy recalls than last 4yrs combined 01/04 California declares state of emergency 01/04 Winter warmth sets records eastern US 01/04 Ohio bans 'gas station heroin' 01/04 World's first vaccine for honeybees	01/04 Health officials' concern: new Covid variant 01/04 Govt. settles 'dreamer' detention lawsuit 01/04 High winds thru Seattle area; power loss 01/04 Windy, stormy conditions in western WA 01/04 SEA ranks #8 top-performing global airports
Cyber, Tech Awareness Go to articles	01/05 Evolving tactics of Vidar stealer 01/05 Anonymous: Serbia is 'Putin's puppet' 01/05 Slack's GitHub code repositories stolen 01/04 Toyota discloses data breach 01/04 The Guardian suffers ransomware attack 01/04 Hack halts Martinique search for new flag 01/04 Cops hacked thousands of phones: legal?	01/05 Play used new method in Rackspace attack 01/04 Healthcare disruptions rise 01/04 Five Guys suffers data breach 01/04 Wrongly jailed: facial recognition error 01/04 US moves to seize FTX digital accounts 01/04 Twitter leak: records of 235M accounts 01/04 December disclosures ransomware victims 01/04 Critical flaws in popular automaker vehicles	01/04 Internet access inequities Seattle, Portland
Terrorism, Extremism Go to articles	01/05 Taliban: anti-terror raids target IS militants 01/04 Group alliance threatens Pakistan leaders	01/04 Far-left extremist groups in the US 01/04 DHS: domestic extremism southern border 01/04 DA: machete suspect wanted jihad on cops	01/03 USAO: 'this is a crime of terrorism'
Suspicious, Unusual Go to articles	01/05 UK's hottest-ever year in 2022 01/04 World's largest dam water level record low	01/04 Expected AFM surge in kids didn't happen 01/04 NFL player's cardiac arrest on football field	
Crime, Criminals Go to articles	01/05 Tech breakthrough nabs serial child abuser 01/04 France: $24M illegal drugs N. Arabian Sea	01/05 Genetic genealogy nabs Idaho suspect 01/04 FBI directed cops to pull over suspect 01/04 Police traffic stop Idaho suspect twice 01/04 'Varsity Blues' mastermind jailed 42mo. 01/04 Baltimore shooting: teen killed, 4 injured 01/04 Virginia shooting: 1 dead, 4 teens injured 01/04 Utah: family of 8 found fatally shot in home 01/04 CBP: $9.1M cocaine Puerto Rico ferry boat 01/04 Reward: $500,000 D.C. pipe bombs case 01/04 Fraudsters stole, spent pandemic money 01/04 CBP South Texas $436M illegal drugs 2022	01/04 Armed robbery spree: 15yr-old, 21yr-old 01/04 Arrest: fire set at Seattle museum facility 01/04 Credit union closes 2 Seattle sites: crime 01/04 Bail fund aided man now murder suspect 01/04 Police: 'Office Space' inspired theft scheme

Events, Opportunities

Top of page

HEADLINE	01/04 Cuban migrants overwhelm Florida Keys
SOURCE	https://www.latimes.com/world-nation/story/2023-01-04/cuban-migrants-flow-into-florida-keys
GIST	MARATHON, Fla. — More than 500 Cuban immigrants have come ashore in the Florida Keys since the weekend, the latest in a large and increasing number who are fleeing their country and stretching thin U.S. border agencies both on land and at sea. It is a dangerous 100-mile trip from Cuba in often rickety boats — many travelers having perished over

the years — but more Cubans are taking the risk amid deepening and compounding political and economic crises at home. A smaller number of Haitians are also fleeing their country's economic and political woes and arriving by boat in Florida.

The U.S. Coast Guard tries to interdict Cuban migrants at sea and return them. Since the U.S. government's new fiscal year began Oct. 1, 2022, about 4,200 have been stopped at sea — or about 43 a day. That was up from 17 per day in the previous fiscal year and just two per day during the 2020-21 fiscal year.

But an unknown number have made it to land and will probably get to stay.

"I would prefer to die to reach my dream and help my family. The situation in Cuba is not very good," Jeiler del Toro Diaz told the Miami Herald shortly after coming ashore Tuesday in Key Largo.

Dry Tortugas National Park, a group of seven islands 70 miles west of Key West, remained closed to visitors Wednesday as the U.S. evacuated migrants who came ashore there.

In Marathon, some 45 miles northeast of Key West, about two dozen migrants were held in a fenced area outside a Customs and Border Protection station where tents had been erected to provide shade. When Associated Press journalists tried to speak with the people through the fence, Border Patrol employees told them to leave.

Ramón Saúl Sanchez with the Cuban American group Movimiento Democracia said he met a group of 22 Cubans who were standing along a main road, waiting for U.S. authorities to pick them up. He and Keys officials said the Biden administration needs a more coordinated response.

"There is a migration and humanitarian crisis, and it is necessary for the president to respond by helping local authorities," Sanchez said.

Cubans are willing to take the risk because those who make it to U.S. soil almost always get to stay, even if their legal status is murky. They also arrive by land, flying to Nicaragua, then traveling north through Honduras and Guatemala into Mexico. In the 2021-22 fiscal year, 220,000 Cubans were stopped at the U.S.-Mexican border, almost six times as many as the previous year.

In Cuba on Wednesday, the U.S. reopened visa and consular services at its Havana embassy for the first time since a spate of unexplained health incidents among diplomatic staff there in 2017 prompted a sharp reduction in American diplomatic presence.

Callan Garcia, a Florida immigration attorney, said most Cubans who reach U.S. soil tell Border Patrol agents they can't find adequate work at home, so they are flagged as "expedited for removal" for entering the country illegally. But the connotation that they will be removed quickly, or at all, is misleading.

Because the U.S. and Cuba do not have formal diplomatic relations, the American government has no way to repatriate them. Cubans are released but given an order that requires them to contact federal immigration authorities periodically to confirm their address and status. They are allowed to get work permits, driver's licenses and Social Security numbers, but cannot apply for permanent residency or citizenship.

Garcia said that can last for the rest of their lives; some Cubans who came in the 1980 Mariel boat lift still are designated "expedited for removal."

"They're just sort of here with a floating order for removal that can't be executed," Garcia said.

A small percentage of Cuban immigrants tell Border Patrol agents they are fleeing political persecution and are "paroled," Garcia said. Under the 1966 Cuban Adjustment Act, they are released until they can appear before an immigration judge to make their case. If approved, they can receive permanent residency

	and later apply for citizenship. On the other hand, Haitian immigrants almost always get sent back, even though political persecution and violence are rife there, as is severe economic hardship. “That inconsistency [is] something that immigrant rights advocates have always pointed to,” Garcia said.
Return to Top	

HEADLINE	**01/04 LAPD secretive private funding arm**
SOURCE	**https://www.latimes.com/california/story/2023-01-04/lapd-police-foundation-private-funding-arm**
GIST	The Los Angeles Police Department and its multibillion-dollar budget were under intense public scrutiny in the spring of 2020. The COVID-19 pandemic had greatly reduced city revenue amid some of the largest and most destructive street protests in decades. The LAPD was being accused of exacerbating the unrest and bungling its response. Activists and politicians were calling for the department’s funding to be slashed in favor of social services for the homeless, mentally ill and poor. Behind closed doors, the money from private donors kept coming. “I wanted to share that since May 28th, we have received more than $48,000 in online donations in support of the Department — a record for our organization and unlike anything we’ve ever seen,” Dana Katz, head of the private Los Angeles Police Foundation, wrote in a June 9, 2020, email to LAPD Chief Michel Moore. Katz wrote to Moore again a couple of weeks later, this time with a list of donors who would be taking part in an exclusive call with him that she had arranged. Katz told Moore it “would be great” if he would brief the philanthropists and corporate bigwigs on the recent protests, the department’s plans for reform and the potential negative effects of “defunding” the police. Moore responded with a simple “thanks.” It wasn’t the first time Katz had tapped Moore for a fundraising initiative. The 25-year-old Los Angeles Police Foundation enjoys regular access to top LAPD officials, working closely with them to craft fundraising campaigns and host meetings with L.A.’s mega-rich and other philanthropic and corporate donors, a Times investigation has found. Just as politicians spend quality time with big campaign contributors, Moore and other police officials regularly assist the foundation. In the quest to secure private cash for the LAPD, they make the case to potential donors that the agency’s already robust taxpayer-funded budget is insufficient for its needs, according to thousands of pages of emails and other public records obtained by The Times. The foundation’s donors are rarely disclosed publicly, although they have an effect on how the LAPD provides for public safety, with a majority dictating how the department can spend the money they give. Since the rise of the “defund the police” movement in 2020, such nonprofits have faced criticism nationwide. The L.A. foundation is no exception. On a near-weekly basis, local activists call in to virtual meetings of the Los Angeles Police Commission — the LAPD’s civilian oversight board, members of which have also worked with the foundation — to lambaste it for approving foundation-funded initiatives. They allege that the foundation’s donors are buying influence and special treatment from the LAPD — or at least trying to — by providing it with expensive technology and equipment that the agency uses to disproportionately surveil and harass communities of color.

Police officials, foundation leaders, donors and their supporters reject those claims as baseless attacks from a radicalized left that threatens to undermine public safety by stripping resources from law enforcement. If anything, they say, private funding for the LAPD reduces the amount of public funds that are designated for law enforcement and helps pay for cutting-edge training and crime-fighting technology.

Moore and Katz acknowledge their close working relationship but say they follow strict ethical standards and all applicable nonprofit laws. They say donors do not receive special treatment.

“My integrity, the integrity of this organization and the integrity of the LAPD — because it reflects on us — are of the utmost importance,” Katz said. “There’s no quid pro quo.”

Katz said that the foundation raises funds for the Police Department so Moore and other LAPD leaders don’t have to and that it never relies on them to solicit money on its behalf.

“If you carry a badge and a gun, you shouldn’t be asking for money,” she said.

Moore noted the same “bright line,” saying he and other LAPD commanders “provide information” to foundation donors, including about financial hurdles the department is facing, but never solicit money directly.

“Our ethics are unbending,” Moore said. “We do not go and ask people for money.”

But LAPD and foundation records obtained by The Times show Moore and Katz working in tandem to raise private funds for the department. They also reveal a robust and successful operation, led by some of L.A.’s wealthiest residents and biggest names, to raise private and often anonymous funding for the largest police agency in the western United States.

It’s a powerful — yet far less public — counterpoint to the local defund movement.

How it works

The Los Angeles Police Foundation was launched in 1998 at the urging of then-Chief Bernard Parks and his wife, who helped it get off the ground by modeling it after organizations in New York and New Orleans.

It has been embraced by every LAPD chief since and, to date, has donated more than $45 million to the department, according to its 2021 tax forms.

The foundation’s donations represent a small portion of the LAPD’s annual budget of more than $3 billion, of which more than 95% goes toward salaries and other personnel costs. But they represent a larger percentage of LAPD spending on advanced training, technology and equipment.

All donations from the foundation to the LAPD must be approved publicly by the Los Angeles Police Commission, and every donation exceeding $17,906 must also go before the City Council. But the people, corporations and nonprofits providing the underlying funding are rarely disclosed during that process.

The commission and council routinely rubber-stamp donations without providing a public accounting of who is behind them, and the foundation has consistently refused to release its donor list.

In 2019, Katz denied a Times request for all donors who had given $1,000 or more and declined to say whether any had earmarked their donations for particular causes. She cited the foundation’s “obligation to protect and respect” its donors’ privacy.

The foundation again denied a Times request for a list of donors in August 2021. That same month, The

Times filed a public records request with the LAPD for years of emails between Katz and police officials, which turned up more than 7,200 pages.

The first set of records, released to The Times in October, not only revealed private conversations between police and foundation officials but included financial filings, fundraising strategies and incomplete lists of donors and their past contributions or pledges.

Some of the biggest givers include Steve Ballmer, the former Microsoft chief executive and owner of the Clippers, and Tony Pritzker, scion of the prominent Pritzker family, whose interests include Hyatt Hotels Corp. Other major donors include Jeffrey Katzenberg, the DreamWorks co-founder and Hollywood producer, and Casey Wasserman (grandson of the late movie mogul Lew Wasserman), another entertainment executive who is president of the Wasserman Foundation and chair of the organizing committee for the 2028 Summer Olympics in L.A.

A representative of Ballmer's philanthropic organization, the Ballmer Group, said it has funded projects aimed at improving public safety, including Community Safety Partnership teams, which prioritize collaboration between LAPD officers and community members in neighborhoods hit by violence. (The Ballmer Group also is helping fund the Los Angeles Times' new early childhood education initiative, a two-year program for which The Times' newsroom retains complete editorial control.)

A spokeswoman for Pritzker said he had no comment on his donations. Neither Katzenberg nor Wasserman responded to requests for comment.

The emails also show efforts to solicit support from wealthy Angelenos.

In February 2020, Katz wrote an email to Moore with the names and contact information of more than a dozen people whom a consulting firm working for the foundation had determined Moore should call directly — "to introduce yourself and ask if you can meet with them to talk about the state of the Department and your vision/goals."

At the top of the list, which Katz said was "in order of priority," was Wallis Annenberg, president and chief executive of the Annenberg Foundation. Second was Walter Wang, chairman and CEO of JM Eagle Inc., the world's largest manufacturer of plastic pipe. According to 2021 tax records, both serve on the foundation's board.

Next on the list were Rick Caruso, the developer and former police commissioner who just spent more than $100 million of his own money on a failed attempt to become L.A.'s mayor, and his wife, Tina. There too were Jeanie Buss, controlling owner and president of the Lakers, and Lakers legend Magic Johnson and his wife, Cookie.

Ted Sarandos, the CEO of Netflix, and his wife, Nicole Avant, were also listed. Avant — daughter of music mogul Clarence Avant, known as the "Black Godfather," and philanthropist Jacqueline, who was murdered in 2021 — is an investor and was U.S. ambassador to the Bahamas in the Obama administration.

None responded to requests for comment, and it is unclear whether Moore followed through on calling them or if they donated to the foundation as a result.

Moore and Katz said not every potential meeting they discussed by email took place.

The effects on policing

The foundation has had a major impact on the LAPD over the years — in many cases championing progressive causes that reflect the politics of its biggest donors and helping to keep the department at the forefront of policing trends.

For example, the foundation in 2008 stepped in with more than $1.4 million in private funding to help

clear a backlog of thousands of untested rape kits that the LAPD had kept in storage freezers for years.

In 2015, it provided nearly $2 million for the LAPD to purchase its first officer body cameras, advancing a program, now publicly funded, that provides greater transparency around police actions, including shootings. It has spent nearly $1.6 million in recent years to bankroll the Community Safety Partnership program.

In 2020, the foundation spent $350,000 to fund an outside review of the LAPD's handling of mass protests following the murder of George Floyd and another $350,000 to hire a marketing firm to help the department improve its recruitment of female, Black and Asian and Pacific Islander officers. It also spent about $600,000 replacing the LAPD's downtown Memorial for Fallen Officers.

In 2021, the foundation donated nearly $1.6 million for a virtual-reality training system with which officers can practice de-escalation and other alternatives to using force. Last year, the foundation donated $1 million to begin rolling out Active Bystandership for Law Enforcement training, which teaches officers to intervene when they witness their peers using excessive force.

The foundation says it has a policy against funding basic training, salaries, police vehicles, weapons or ammunition. Between major projects and campaigns, it funds smaller events aimed at boosting officer morale, such as holiday parties, and equipment purchases for individual units, such as binders to help homicide detectives keep case files organized.

The foundation also funds big-ticket technology and equipment purchases that the city is unwilling or unable to make.

In November, activists objected to a donation of nearly $278,000 for a robot that can open doors, climb stairs and help flush suspects from homes. Officials said the robot would be deployed to assist the department's SWAT team in carrying out high-risk search warrants and apprehending barricaded suspects; activists said it was military equipment that has no place in city policing.

The foundation has also helped the LAPD purchase drones, closed-circuit cameras and data analytics software that officials say are used ethically and sparingly but activists say are wildly intrusive and used disproportionately in communities of color.

Hamid Khan, a regular critic of the LAPD and a coordinator with the Stop LAPD Spying Coalition, said the foundation over the years has helped the department build a dystopian network of surveillance capabilities by paying for equipment purchases that would have raised more questions had they been publicly funded.

Khan cited as one example the LAPD's purchase years ago of Palantir data analytics software, for which the foundation contributed $178,000 in funding from Target Corp., Katz said. The software was used as part of a "predictive policing" program that attempted to identify "chronic offenders" and crime hot spots for increased attention from law enforcement. But it was discontinued amid concerns that it lacked oversight, used inconsistent criteria to label alleged or potential offenders and unfairly targeted Black and Latino communities.

Target has since stopped donating to the foundation.

Khan said donations to the LAPD from private individuals and corporations at the very least give the appearance of impropriety — suggesting that deep-pocketed interests can buy favor with law enforcement or help set the approach to policing.

"We have to be really looking at it in a very critical way," he said.

Kandyce Fernandez, an assistant professor of public administration at the University of Texas at San Antonio who has studied private funding of police departments, said L.A. is no outlier.

She and a research colleague recently counted more than 250 similar foundations nationwide, she said. The number surged starting in 2010, when many cash-strapped cities were looking for lifelines amid the Great Recession.

However, the Los Angeles Police Foundation is one of the biggest such groups in the country. And it is by far the largest private donor to the LAPD, according to a 2020 audit by the department's inspector general, providing $6.6 million of the $9.4 million in total donations the LAPD received in 2019.

Such funding, Fernandez said, raises questions about equity, when richer areas attract more funding, and about transparency, when the people, corporations or nonprofits behind the donations aren't disclosed.

Big business and other benefactors

Emails between the LAPD and foundation officials show that in addition to individual philanthropists, the foundation has received funding from companies that have interests in the city and do business directly with the department — at times with its help.

For example, in May 2019, Katz wrote an email to Moore's chief of staff, then-Department Chief Robert Green, saying she was "working on securing sponsorships" for the foundation's annual "Above and Beyond" fundraiser, which honors officers for bravery in the field.

"Is it possible for the Department to put together a list of its top 10-15 vendors (with contact names and email addresses, if available) for me to reach out to?" Katz asked.

"Happy to provide them," Green replied.

Four months later, the event's main sponsor was Motorola Solutions, which does substantial business with the LAPD and has held a master service agreement for telecommunications work with the department since 2014. That contract was renewed in February for nearly $9.5 million.

Other event sponsors included Axon, maker of the LAPD's body cameras and other technology; Glock Inc., which has sold pistols to the department; and Ring, the Amazon-controlled manufacturer of security cameras that once tapped LAPD officers to hawk its products to residents.

The Times found no evidence that the donations influenced contract decisions.

Neither Motorola nor Glock responded to requests for comment. Axon, in a statement, said it sees supporting the Los Angeles Police Foundation as a means of supporting "the broader community" and is "committed to doing business transparently" but declined to tell The Times how much it has donated.

Ring, which donated $10,000 to the 2019 "Above and Beyond" event, no longer works with the LAPD to sell its products and said in a statement that it has stopped donating to law enforcement organizations. Some of the foundation's biggest donors are other foundations and nonprofits.

Ballmer Group has been a major funder of body cameras and the Community Safety Partnership program. In just one example, it gave $250,000 in 2020 for a CSP site in the South Park neighborhood.

The Ahmanson Foundation, a major philanthropic body founded in the 1950s in L.A. County by financier Howard Ahmanson and his wife, Dorothy, has donated many times — including a $5-million contribution toward a recent foundation campaign to replace aging LAPD technology systems.

Bill Ahmanson, the group's president, said it assesses requests for funding from the Los Angeles Police Foundation just as it does requests from any other potential beneficiary — by looking at the population that will be served and whether the contribution will be meaningful.

Ahmanson said he sees no problem with police officials like Moore working to attract private funding. "Everybody in this city is trying to raise funds," Ahmanson said. "We always seem to have enough money in the city to do everything we want but never enough money to do anything well."

'I need you to step up'

According to the LAPD and foundation emails obtained by The Times, the foundation has frequently leaned on Moore to meet with major donors and business leaders and lay out the ways in which the department could benefit from private cash.

Despite their claims to the contrary, foundation officials have repeatedly prodded Moore to ask for money directly, and he has skirted that line — if not crossed it.

For example, in April 2020, the foundation was in the midst of a major fundraising campaign to upgrade the LAPD's outdated technology and computer systems. It was also trying to get a handle on the department's needs related to the COVID-19 pandemic.

On April 15, Katz sent Moore a planning memo for a private phone call between him and more than 40 billionaires, millionaires and corporate and nonprofit representatives from the worlds of development, sports, merchandising, private equity, banking, healthcare and entertainment. The memo had been drafted by the consulting firm Gonring Lin Spahn, which the foundation was paying $25,000 a month to help run its tech campaign.

Also on the list was developer Steve Soboroff, who has been criticized by activists for helping to orchestrate donations to the foundation while serving on the Los Angeles Police Commission, of which he is a current member. He also has been pilloried for directing funding to the foundation personally as a former board member of the Weingart Foundation.

Soboroff said in an interview that all of his support has been aboveboard, and he has never been sanctioned for violating city ethics rules.

In addition to the attendee list, the memo provided "suggested talking points" for Wasserman, Katzenberg and Pritzker, the technology campaign's co-chairs, as well as for Moore — advising him to express his desire for more officers on the streets and stress the department's growing financial needs amid the pandemic.

"My budget will likely be cut, which means we need to be thinking about the long term now," read one of the talking points for the chief. "If you want to step up, I need you to step up for this," read a second.

Months prior, Katz had sent Moore talking points for a planned one-on-one call with Peter Guber, chairman and chief executive of Mandalay Entertainment and co-owner of the Dodgers and Golden State Warriors. That memo proposed that Moore ask Guber to donate $1 million and join Wasserman, Katzenberg and Pritzker as a technology campaign co-chair.

"Right now, all the Co-Chairs of the Capital Campaign have committed $1 million," one of the talking points for Moore read. "I know all of us couldn't imagine leading this effort without you."

Guber did not respond to a request for comment.

In interviews with The Times, Moore stood by his claim that he has never solicited money for the foundation. He said he has appreciated the "talking points" from foundation leaders but never followed them when they crossed his "bright-line standards" against soliciting funds.

Moore has given the foundation permission to raise funding by granting naming rights to an LAPD facility and provided guidance on opposing any cuts to public funding.

At one point in 2020, Katz emailed Moore about selling naming rights to public LAPD facilities — in

part because Pritzker wanted to give $1 million to put his name where rank-and-file officers would be sure to see it.

“I spoke with Tony Pritzker’s foundation head, and his primary priority is visibility with the officers,” Katz wrote. “In looking at the opportunities for $1M gifts, I thought that one of the [Elysian Park] ranges would be best, but I would welcome your thoughts/opinion.”

“This is fine,” Moore wrote back. “I support.”

Today, LAPD officers receive combat training at the Pritzker Combat Range.

Judy Schroffel, Pritzker’s senior executive assistant, said Pritzker had no comment on the deal.
Later that year, the LAPD — like every other city department — was facing potential budget cuts due to massive revenue shortfalls related to COVID-19.

Again, the foundation got to work, the records show, discussing with Moore an organized campaign to get business leaders to reach out to city officials — including then-Mayor Eric Garcetti and members of the City Council — to oppose cuts to police.

On Dec. 9, 2020, Katz emailed Moore a list of business leaders with the Valley Industry & Commerce Assn. who were meant to be on a call with him to hear about the effects of budget cuts on public safety in the San Fernando Valley.

“I am sure they will have questions and are looking for a call to action, which I’ve told them will be primarily to contact the city councilmembers and mayor to urge them not to adopt the cuts,” Katz wrote.
“Thank you!” Moore wrote back. “Good group.”

Stuart Waldman, the group’s president, said he had requested the meeting because group members were “really concerned” about police budget cuts. During the meeting, he said members “expressed overwhelming support” for the LAPD and urged him to “put out an action alert” to other members, which he did.

About a week later, on Dec. 18, Dwayne Gathers of the Hollywood Chamber of Commerce wrote to Katz, saying he and other board members were “ready to engage” in opposing LAPD cuts, including by getting chamber businesses and their employees to voice opposition.

Katz forwarded the note to Moore, who responded, “Thanks!! Sounds like progress.” He then suggested that a written campaign — in the form of letters to the editor or opinion editorials in local news outlets — could be helpful.

Moore said naming the combat range after Pritzker was a “tribute” to his generosity to the department. He said he has always been candid with local business leaders about the needs of the department and at times encouraged them to make their voices heard by speaking with their elected representatives.

The future of giving
LAPD officials for years have been defending the agency against critics of private funding.

Following its audit of donations in 2020, the LAPD inspector general’s office recommended that the department improve its tracking and documentation of donations, improve its process for assessing whether donations raise conflicts of interest and “set forth appropriate parameters limiting special access for donors to Department personnel and/or facilities.”

The audit had found, among other issues, that despite an LAPD policy barring donors from receiving preferential treatment, half a dozen foundations raising private funding promised just that — telling donors that “a certain level of donation would ensure a meeting” with LAPD commanders or that small contributions could get them “tours of Area stations or some other sort of unique Department access or

	experience." The audit did not specify whether the Los Angeles Police Foundation was among those promising special access, though the records obtained by The Times show that it was providing donors with such access through its exclusive meetings with Moore. Recommendations aside, the inspector general concluded that the LAPD's overall process for receiving donations was "generally well designed." In a recent interview, William Briggs, an attorney and president of the Los Angeles Police Commission, said the foundation is doing good work in L.A., citing as an example the recent $1-million donation for active bystander training — which he said will "change the culture of the LAPD" for the better. "If the city could fully fund the LAPD, there is no doubt that it would. But until such time as this can happen, the foundation assists with maintaining the LAPD at the level of a world-class police department," Briggs said. "I am grateful for their commitment." Soboroff — who has long helped the foundation raise funds, most recently for a program to offset housing costs for new officers — said any criticism of the group is misplaced. He said no one who donates or is otherwise involved with the foundation "receives or asks for favors," and he has never seen anything untoward occur — from either its leaders or police commanders — over decades of observing its work. Soboroff said it would make sense for companies that have contracts with the city or the LAPD to publicly disclose contributions to the foundation as a matter of transparency, even though he said such contributions have no impact on contract decisions and should be allowed to continue. But, he said, he understands why some private donors want to remain anonymous — and supports their ability to do so — given the atmosphere around policing. He said he has received death threats from activists for his work on the commission — which is exactly what donors fear. "You want to look at my emails? You want to see the security I have?" Soboroff said. "I don't blame them one bit."
Return to Top	

HEADLINE	**01/05 Ukraine pleads for tanks from allies**
SOURCE	**https://www.reuters.com/world/europe/russia-blames-its-soldiers-mobile-phone-use-deadly-missile-strike-2023-01-03/**
GIST	KYIV, Jan 5 (Reuters) - Ukrainian and Russian troops battled in eastern regions on Thursday as Kyiv tried to push back occupying forces, while President Volodymyr Zelenskiy urged the West to provide his army with heavy tanks to boost their firepower. The Ukrainian military said the Russians were focused on an offensive in the Bakhmut sector of the Donetsk region, but their attacks in the Avdiivka and Kupiansk sectors were unsuccessful. The governor of neighbouring Luhansk region, meanwhile, said Ukrainian troops were recapturing areas there "step-by-step" but cautioned it was "not happening fast". Luhansk and Donetsk make up the Donbas region, Ukraine's industrial heartland, parts of which were seized by Russian-backed proxies in 2014. Russia declared Donetsk, Luhansk, Kherson and Zaporizhzhia regions as part of its territory in September after referendums condemned by Ukraine and Western countries. Russia does not fully control any of the four regions.

Bakhmut, which is now largely in ruins after months of battering by Russian artillery, is important because the Russian leadership wants to have a success to hold up to the Russian public after a series of setbacks in the war.

It is located on a strategic supply line between the Donetsk and Luhansk regions. Gaining control of the city, with a pre-war population of 70,000-80,000 that has shrunk to close to 10,000, could give Russia a stepping stone to advance on two bigger cities - Kramatorsk and Sloviansk.

Fighting has been particularly tough there, with commanders on both sides describing it as a "meat grinder".

Ukraine's military said it estimated 800 Russian soldiers were killed in the past day, mostly in fighting in Donetsk. The figure - which would signify a huge loss of life for a single day - could not be independently confirmed.

The Luhansk governor, Serhiy Haidai, said he expected fighting to intensify across the eastern front as temperatures drop further and the ground freezes.

"Then the opportunity to use heavy equipment will open up," he said.

HEAVY WEAPONS
A senior U.S. administration official also predicted a long road ahead in the war that has now raged for nearly 11 months.

"The fighting is still quite hot (in Donetsk)...what we're seeing in Bakhmut we should expect to see elsewhere along the front, that there will be continued fighting in the coming months," the official said in Washington on Wednesday.

In his evening video address on Wednesday, Zelenskiy urged Western allies to provide his army with tanks and heavy weapons to combat the Russian forces.

French President Emmanuel Macron said on Wednesday his government would send light AMX-10 RC armoured combat vehicles to help its war effort.

Zelenskiy thanked Macron but said: "There is no rational reason why Ukraine has not yet been supplied with Western tanks."

The Ukrainian leader also said his troops outside Bakhmut were inflicting numerous losses on their adversaries and Russia was building up its forces in the region.

Russian air, missile and rocket attacks on Bakhmut and two other cities in Donetsk - Kostiantynivka and Kurakhove - had caused an unspecified number of civilian casualties, Ukraine's military said.

Russia denies targeting civilians in what it calls its special military operation in Ukraine.

Luhansk governor Haidai, asked on national television about the possibility of a Ukrainian counteroffensive in that region, said the cities of Rubizhne and Sievierodonetsk had been destroyed by Russian occupation forces and could no longer be used as strongholds.

"But we should not forget that there is also the defence line, which they (Russian proxies) have been building since 2014 - the occupiers have very fortified positions there. Therefore, it will not be easy to liberate the Luhansk region," he said.

Russia was sending in extra troops, including conscripts, Haidai added.

	Yegeny Balitsky, the Russian-installed governor of the Russian-held Zaporizhzhia region in the southeast, said Ukrainian artillery killed five people and wounded 15 including four emergency workers, Russia's TASS news agency reported. Reuters could not independently verify battlefield accounts. APPEAL FOR TANKS As the war grinds on, the Kyiv government has repeatedly asked Western allies for heavier fighting vehicles such as the Abrams and German-made Leopard tanks. U.S. President Joe Biden said on Wednesday the United States was considering sending Bradley Fighting Vehicles to Ukraine. The Bradley has a powerful gun and has been a U.S. Army staple to carry troops since the mid-1980s. Biden's decision, however, would fall short of sending the Abrams tanks that Ukraine has sought. The United States is preparing another package of weapons, which could be announced in coming days on top of about $21.3 billion in security assistance so far to Ukraine. The United States has increased the capability of the weapons it has sent including shoulder-fired Stinger anti-aircraft missiles as well as Javelin anti-tank missiles, the HIMARS rocket system and NASAMS surface-to-air missiles. During a visit by Zelenskiy to Washington last month, the United States pledged to send the Patriot missile system to repel Russian missile and drone attacks. Russia launched its invasion on Feb. 24, citing threats to its security and a need to protect Russian speakers. Ukraine and its allies accuse Russia of an unprovoked war to seize territory.
Return to Top	

HEADLINE	**01/04 Oil falls; mounting global economic worry**
SOURCE	**https://www.newsmax.com/finance/streettalk/oil-prices-energy-global-economy/2023/01/04/id/1103014/**
GIST	Oil fell by more than $3 a barrel on Wednesday after slumping in the previous session, weighed down by demand concerns stemming from the state of the global economy and rising COVID cases in China. Brent futures fell $3.53 to $78.57 a barrel for a 4.3% loss by 11:39 a.m. EST (1639 GMT). U.S. crude dropped $3.37, or 4.4%, to $73.56. Both benchmarks also plunged more than 4% on Tuesday, with Brent posting its biggest daily decline in more than three months. "Worries about the state of the global economy are front and center of traders' minds and will remain so for the foreseeable future," said PVM Oil analyst Stephen Brennock. The head of the International Monetary Fund warned that much of the global economy would face a tough year in 2023 because activity was weakening in all three main engines of global growth, the United States, Europe and China. U.S. manufacturing contracted further in December, dropping for a second straight month to 48.4 from 49.0 in November, in the weakest reading since May 2020, the Institute for Supply Management (ISM) said. At the same time, a survey from the U.S. Labor Department showed job openings fell 54,000 to 10.458 million on the last day of November, raising concerns that the Federal Reserve would use the tight labor market as a reason to keep rates higher for longer. Also dampening oil prices was data out of China showing that while no new variant has been found there,

	the country also under-represents how many people have died in its recent rapidly spreading outbreak, World Health Organization officials said. The Chinese government increased export quotas for refined oil products in the first batch for 2023, signaling expectations of poor domestic demand. Top oil exporter Saudi Arabia could cut prices for its flagship Arab Light crude grade to Asia in February, having been set at a 10-month low for this month, as concern about oversupply continued to cloud the market. OPEC oil output rose in December, a Reuters survey found on Wednesday, despite an agreement by the wider OPEC+ alliance to cut production targets to support the market. The Organization of the Petroleum Exporting Countries (OPEC)pumped 29 million barrels per day (bpd) last month, the survey found, up 120,000 bpd from November. U.S. crude oil stockpiles are likely to have risen by 2.2 million barrels, with distillate inventories expected to have fallen, a preliminary Reuters poll showed on Monday. Industry group American Petroleum Institute is due to release data on U.S. crude inventories at 4.30 p.m. EDT (2030 GMT) on Wednesday. The Energy Information Administration will release its figures at 10.30 a.m. (1430 GMT) on Thursday.
Return to Top	

HEADLINE	**01/04 Manufacturing weakens on easing demand**
SOURCE	**https://www.newsmax.com/finance/streettalk/u-s-manufacturing-output-economy/2023/01/04/id/1103001/**
GIST	U.S. manufacturing activity contracted for a second month in December, remaining at the lowest levels since May 2020 as new orders and production slipped, survey data showed Wednesday. The world's biggest economy has been squeezed by decades-high inflation, prompting the central bank to raise interest rates multiple times in an all-out campaign to ease demand and rein in cost increases. While the domestic economy has largely held up, there are growing signs the Federal Reserve's policy moves are rippling through sectors -- adding to broader factors like slowing global activity. The Institute for Supply Management's (ISM) manufacturing index dipped 0.6 points to 48.4 percent in December, according to data released Wednesday. This was similar to analyst expectations, and the reading remains firmly below the 50 percent threshold indicating growth. The manufacturing Purchasing Managers Index also remains at its lowest level since the coronavirus pandemic recovery began, said ISM manufacturing survey chair Timothy Fiore in a statement. The latest reading "offers more evidence that the days of heady growth are behind us," said economist Oren Klachkin of Oxford Economics, adding that a pandemic-driven hot streak in manufacturing ends this year. "Tighter financial conditions and a weaker labor market will cramp domestic goods demand, and the strong greenback and soft external demand will weigh down exports," he added. For now, ISM's Fiore said with respondents "reporting softening new order rates over the previous seven months," December's index reflects that companies are slowing their output. The new orders index remains weak, data showed, and the production index fell into contraction.

	While supplier deliveries has improved, "companies continue to judiciously manage hiring," Fiore added. The employment index has picked up, but many firms confirm that they are still managing headcount through hiring freezes, employee attrition and layoffs, the report said. "Customer demand continues to be depressed," according to a survey respondent in the chemical products sector. "While 2023 pipeline is looking very positive, current demand is significantly down," the firm added. Other participants reported skilled labor shortages and continued uncertainty in the economy.
Return to Top	

HEADLINE	**01/04 Power grids under assault**
SOURCE	**https://www.forbes.com/sites/craighooper/2023/01/04/with-electrical-grids-under-assault-us-and-ukraine-seek-scarce-transmission-gear/?sh=75e1de15325f**
GIST	Russia, eager to break Ukraine's power grid, is subjecting Ukrainian electrical substations to a withering array of missile and drone strikes. A simultaneous rise in physical attacks on U.S. electrical substations risks advancing Russian war aims by crimping the already tight global supply of transformers and other key electrical grid subcomponents. Assaults on America's sprawling electrical infrastructure are on the increase—at least 19 attacks have occurred since September alone. With electrical transmission equipment supplies at critical lows, American utilities are scrambling to prepare for more attacks—and trying to boost their supply of electrical transmission parts just as Ukraine is hunting for the very same electrical supplies. The limited global supply of electrical distribution equipment is a well-known global bottleneck. Electrical utilities have been struggling with electrical distribution equipment supply chain issues for years. Transformers—oil-filled structures that step voltage up or down—have been in critically short supply due to strong demand, and the COVID-19 pandemic, labor constraints and shipping issues haven't helped. Russia's invasion, and Ukraine's scramble to recover from Russian attacks on critical electrical infrastructure, has already pushed transformer inventories to record lows and radically increased transformer prices worldwide. Continued attacks on electrical grids far away from the Ukraine battlefield could push the already-stressed electrical distribution equipment market into disarray, making it even harder for Ukraine to keep the lights on. **For Russia, Power Disruption Is A Strategic Priority** While those responsible for the latest wave of U.S. power grid attacks are largely unknown, Russia has made no secret that it considers electricity generation and distribution to be a target, and has signaled for months that power and electrical generation was a primary facet of Russian strategy. In October, in response to complaints about Russian attacks on Ukrainian critical infrastructure, Russian President Vladimir Putin warned that "any critical infrastructure in transport, energy or communication infrastructure is under threat—regardless of what part of the world it is located, by whom it is controlled, laid in the seabed or on land." Aside from direct attacks on energy infrastructure in Ukraine, disrupting power grids in other countries offers a logical step to advance Russian war aims. Russia has a lot of options to disrupt electrical networks. Direct Russian attacks on foreign electrical infrastructure, while extremely risky, is certainly not beyond the capability of the Russian government. European governments already suspect that Russia is behind the explosion of two Nord Stream pipelines under the Baltic Sea. And Russians have been caught repeatedly throughout Europe, flying drones over

critical European energy infrastructure.

Anything is possible. With the European Parliament declaring Russia a state sponsor of terrorism in November, and with European officials linking Russian military intelligence to high-profile European assassinations and bombings of ammunition dumps and depots—a record of terroristic violence throughout Europe that started in 2006 with the gruesome use of radioactive polonium to assassinate Alexander Litvinenko in the U.K.—Russia's campaign to break Ukraine's power grid could well extend beyond the battlefield, into Europe and, potentially, into America.

Indirect attacks on energy infrastructure, allowing Russia plausible deniability, are hard to carry out, but they have already occurred in Europe. An hour before the Russian invasion began, collateral damage from an uncontrolled Russian cyber attack disabled thousands of German wind turbines.

But Russia's most viable means of disrupting electrical grids may well come from encouraging or facilitating attacks by others. In the U.S,, observers note that a mix of white supremacists, accelerationists, and other murky criminal elements known to take cues from Russia have been expressing particular interest in attacking U.S. power infrastructure, and are wondering what is converting long-held terroristic ideations into action at this particular time.

Russia has a record of helping dispersed and otherwise disorganized networks coalesce around an activity or a cause. For example, cyber criminals with suspected links to the Russian government have repeatedly attacked energy infrastructure. As early as 2017, researchers at the Henry M. Jackson School of International Studies identified several ties between Russian-government associated cybercriminals and electrical grid attacks.

Coordination is possible. In the run-up to the Russian invasion, some European governments wondered if an increase in cyber attacks on the European power sector was orchestrated by Russian intelligence. But, regardless of motivation, nobody doubts Russian criminals have-and are currently-targeting electrical and power infrastructure in Europe and elsewhere. Russian-based cyber criminals orchestrated the Colonial Pipeline fiasco, disrupting fuel distribution up the East Coast. And other Russian cyber criminals have continued attacking European power companies, hitting one of Germany's largest power distribution companies as recently as October.

The Russian cyber underworld is a murky place, and defining attribution for any cyber attack is a challenge. But investigators are certain Russian cyber criminals have, at times, been linked to Russian intelligence and have worked together. Past collaborations have been both lengthy and recent. A 2021 report from Analyst1, a threat intelligence company, described how two Russian intelligence directorates and ransomware gangs worked "together to compromise U.S. government affiliated organizations between October and December 2020," pointing out close personal relationships between individuals in the criminal organizations and the Russian Federal Security Service as well as identifying interesting parallels between Russian state malware and malware employed by the Russian cybercriminals.

If the breakdown of Ukraine's power infrastructure is a critical facet of Russian strategy, then it is logical to question to what extremes Russia would go to carry it out.

American Extremists Are Obsessed With The Electrical Grid—And Linked To Russia

Just as the Russian government is associated with cyber criminal networks, observers believe the Russian government has developed similar ties to an array of extremist movements—attracting adherents associated with a longer-term, five-year rise in domestic attacks on the U.S. electrical grid.

Again, the extremist underworld is a murky place. But, again, investigators have repeatedly identified Russian links to American adherents of white supremacy and accelerationism. The U.S. State Department designated a Russian group known for offering training to the organizers of the infamous Charlottesville, Virginia white power riots as a terrorist organization. And U.S. intelligence experts even wonder if the founder the white supremacy group "The Base"—a U.S. citizen who now lives in Russia—was a long-time Russian agent.

If Russia has been interested in pushing susceptible Americans into attacking the power grid, the extremist community is certainly primed for it. Talk of disrupting the U.S. power grid has rattled around in U.S.-based white supremacist and accelerationist groups for decades.

But noting nefarious may be going on. Extremists may simply reflect Russian rhetoric and strategic interests. Just as Russia eyed Ukraine and began really tinkering with the idea of using energy as a weapon, white supremacist plots targeting U.S. energy systems "dramatically increased in frequency." Researchers at George Washington University found that, between 2016 and 2022, 13 white supremacists were prosecuted for energy system attacks, with 11 of the attack planners charged after 2020. Concomitantly, attacks and incidents on U.S. electrical critical infrastructure increased, as U.S. attackers apparently began to act on long-simmering terrorist ideations.

It would be easy for Russia to enable domestic extremists to carry out more effective attacks. In 2020, researchers warned that a 14-page handbook calling for attacks on the power grid was being passed around extremist circles on Telegram—an instant messaging system popular in Russia. After the handbook emerged, detailing low-tech means to disrupt the electrical grid, both the frequency and the effectiveness rate of attacks on U.S. electrical transmission infrastructure increased—with thousands of people loosing power.

For Russia, encouraging widespread attacks on overseas electrical transmission infrastructure would be an easy way to exacerbate a global supply shortage in key components needed to ensure a resilient power grid. Even the threat of doing so contracts the global market, making each transformer Russia bombs in Ukraine far harder to fix.

Given U.S. concerns that extremist attackers are following mysterious and murky online cues to shoot up U.S. electrical substations, utilities are scrutinizing their inventories and worrying about their stockpiles of spare parts. Without well-thought out resiliency plans to pre-deploy recovery resources, attacked substations are not easy for utilities to fix. Power outages need to be fixed fast, but electrical equipment is bulky, hard to store, tough to transport and takes time to install. A December 3 shooting attack on two electrical substations in Moore County, North Carolina, left some 40,000 customers in the dark for days. A complex, multi-site attack on Christmas Day cut power to more than 14,000 in Washington State. Even unsuccessful attacks chip away at the resiliency of the grid, raising the stakes for the utility that is targeted.

The number and complexity of attacks and/or "suspect events" at U.S. electric facilities are concerning. USA Today reported that, "since September, attacks or potential attacks have been reported at least 18 additional substations and one power plant in Florida, Oregon, Washington and the Carolinas."

According to a security specialist, the substation attacks in the Northwest included "setting the control houses on fire, forced entry and sabotage of intricate electrical control systems, causing short circuits by tossing chains across the overhead buswork, and ballistic attack with small caliber firearms."

Unhardened transformers are particularly vulnerable to gunfire. As insulating oil leaks from a shot-up transformer, the subsequent rise in temperature can break the transformer, sometimes sparking a catastrophic explosion-catnip for prospective terrorists eager to make some kind of a statement.

Supply Chain Disruption Can Enhance Battlefield Effects

For electrical utilities, transformers are a particular concern. The transformer market in the United States has been tight for more than a decade.

Today, suppliers need two to three years of lead time to replace big transformers (generally transformers are oil-filled structures used to step voltage down or up), and, while transformers do break down, U.S. electrical utilities generally don't carry a large inventory of replacements.

But America's already modest stockpiles of backup electrical transmission gear are getting critically low. One utility company in the northwest noted in June that while they try to keep a supply of 60 mid-sized

transformers on hand "at all times," their inventory had dropped "well below" 20, the minimum required for resilient operations.

The supply of larger transformers is in a similar state. Orders that typically took between 6-12 weeks to fulfill in 2020, now have lead times of 52-86 weeks.

Prices have headed into the stratosphere. By mid 2022, 25kVA pad-mounted transformer prices "rose nearly 400% from 2020 per-unit pricing, and 50kVA unit pricing jumped 900% since 2020."

The tightening supply is a recipe for a conflict between friends. As U.S. electrical utilities scramble for spare transformers and struggle to protect the more than 6,400 power plants and 55,000 electrical substations that backstop America's electrical grid, Ukraine is begging for help and spare parts. And, unsurprisingly, Ukraine's top priority are transformers—the exact same equipment America's electrical utilities need.

The U.S. has certainly scrambled to help, but further attacks may limit the amount of help America can offer. On November 29, just days before the power grid attacks in North Carolina, the U.S. State Department announced $53 million in electrical aid, including "distribution transformers, circuit breakers, surge arresters, disconnectors, vehicles and other key equipment." Aside from the fact that American electrical utilities will be bidding against Ukraine for replacement transformers and transmission gear, it is easy to envision a scenario where U.S. citizens, sitting in the dark after a domestic attack, start wondering why the U.S. is prioritizing electrical assistance for Ukraine.

On a global level, all the components are in place for a catastrophic run on electrical transmission supplies. In the U.S., rationing might even be required if more U.S. attacks encourage more U.S. utilities scramble for more spare parts. Panic can be contagious, and, if other countries start following the U.S. lead, a lack of electrical supplies could be a real blow to the global economy.

The path ahead is clear. U.S. authorities must move far faster to investigate—and catch—any future attackers. In addition, America will have to move quickly to ensure utilities are up to code and, in some cases, working to "harden" vulnerable parts of the Nation's dispersed electrical transmission infrastructure. Behind the scenes, the U.S. must take other steps to both deter extremists and to ensure Russia's efforts to subdue Ukraine are limited to the immediate battlefield.

Efforts to interfere or otherwise compromise the global supply of electrical grid components are unacceptable. Using the vagaries of a fragile global supply chain to exacerbate battlefield aims makes for a tempting strategy, but it is operationally hard to carry out. Nation-state practitioners can suffer unanticipated blow-back, ending up suffering unexpected diplomatic and economic damage. And, in a war, two can play the same game—Ukraine is perfectly capable of targeting Russia's power grid too.

Caution is warranted. But the bottom line is this: however tempting it might be for Russia to exacerbate the impact of their attacks on Ukraine's power grid, foreign attacks on the U.S. power grid—even indirect ones—are warlike acts, that, if detected, will demand a response.

Return to Top

HEADLINE	**01/05 California's 'Pineapple Express' storm**
SOURCE	**https://www.washingtonpost.com/weather/2023/01/05/california-weather-explained-pineapple-express-storm/**
GIST	When extreme weather events occur, puzzling and often ominous terms crop up — "firenado," "polar vortex," "thundersnow." On Wednesday, though, California declared a state of emergency as the latest in a string of storms slammed the West Coast with a name that sounded oddly sunny: "Pineapple Express." The storm, which has brought 100-plus mph wind gusts and could cause flooding and landslides, is no day at the beach, however. So what, exactly, is a Pineapple Express? The powerful storm type gets its name from its origin in the tropical Pacific around Hawaii and the island

	state's affinity for the sweet treat. Pineapple Express storms carry moisture northward from the tropics and dump it in high concentrations on the West Coast and Canada. To make matters worse, this particular storm system is also a rapidly intensifying "bomb cyclone" system (another menacingly named storm referring to the speed at which the air pressure drops). Fueled by a powerful southern portion of the polar jet stream, which is strongest in the winter, according to the American Meteorological Society, the Pineapple Express is sometimes likened to a "conveyor belt" of moisture. It can bring as much as 5 inches of rain a day, the National Oceanic and Atmospheric Administration says. Pineapple Express storms are a particularly well-known type of "atmospheric river," considered a fundamental feature of the earth's water cycle. They can be beneficial — supplying fresh water and even alleviating drought or quelling wildfires — but they can also slam the West Coast and Canada with dangerous amounts of snow and rain. Scientists have cautioned that they could worsen amid climate change. These rivers in the sky can stretch thousands of miles long and are often just a few hundred miles wide. The largest freshwater "rivers" in the world, they can carry more than twice the volume of the Amazon. They occur elsewhere, too — in the United Kingdom and the Iberian Peninsula, for example, which receive moisture from the Caribbean. In February, Brisbane, Australia, received 80 percent of its typical yearly rainfall in three days from an atmospheric river. Similar to hurricanes, atmospheric rivers are ranked from 1 to 5. The scale — which goes from "primarily beneficial" to "primarily hazardous" — corresponds to how much moisture they transport as well has how long they last in a particular area. The rating system wasn't developed until 2019. On Wednesday, the Center for Western Weather and Water Extremes forecast that the coming Pineapple Express would reach Category 3, a "strong" event, in the San Francisco Bay area. In the coming days, it could increase to a 4, but the organization cautions that it is difficult to make predictions too far out. While California is known for its long dry spells, the Golden State is no stranger to such weather events. Researchers found that from 1979 to 2019, atmospheric rivers of varying intensities hit the West Coast an average of 24 times per year. In October 2021, one brought California some relief, following a record-breaking dry period. And atmospheric rivers have been hitting the region again in recent weeks. In December, such events poured 11.6 inches of rain on San Francisco, The Washington Post reported. Scientists have projected that such weather whiplash — dry to wet precipitation events — could increase by 25 to 100 percent in California by the end of the century. And as the planet warms, atmospheric rivers could get wider, longer and more intense, studies have suggested.
Return to Top	

HEADLINE	**01/05 NKorea drone near Seoul presidential office**
SOURCE	**https://www.washingtonpost.com/world/2023/01/05/north-korea-drone-seoul-president-office/**
GIST	SEOUL — A North Korean drone entered a no-fly zone surrounding Seoul's presidential office last week, South Korea's military said Thursday, in the latest example of the growing military threat from Pyongyang, which has also ramped up missile testing and sent planes near the border. The South's military previously apologized for failing to shoot down North Korean drones that crossed the border Dec. 26 — the first time they had done so in five years — but had denied that the no-fly zone around the top government office was violated in the intrusion. The unmanned aircraft flew over South Korea for five hours, prompting an armed response.

	The Joint Chiefs of Staff reversed the denial on Thursday and said one of the five drones had entered the northern end of the 2.3-mile area. It said the initial analysis was modified after an internal review of the military's readiness posture. The unmanned aircraft did not fly directly over the presidential office in central Seoul's Yongsan district, said Col. Lee Sung-jun, a JCS spokesman. The JCS said separately that the safety of the office had not been compromised. The South Korean military does not have sufficient capacity to detect and intercept surveillance drones that are smaller than 10 feet, though larger and more threatening combat drones can be engaged with more easily, Lt. Gen. Kang Shin-chul, chief director of operations at the JCS, said during a televised briefing last week. The military scrambled fighter jets and attack helicopters to bring down drones that flew over cities including Seoul, the capital and home to some 9 million people. However, they were limited from a more aggressive response because of concerns about civilian safety, Kang said. South Korean President Yoon Suk Yeol, who was briefed Wednesday about countermeasures to the drone intrusion, called for an "overwhelming response capability to North Korean provocations that goes beyond proportional levels." Yoon, a conservative who has given Seoul a more hawkish stance toward Pyongyang since taking office last year, also instructed his defense minister to set up a drone unit and develop anti-drone capabilities, according to presidential spokeswoman Kim Eun-hye. North Korea also fired multiple rounds of ballistic missiles toward the sea last week, capping a record year of weapons tests. The North's leader, Kim Jong Un, called Sunday for an "exponential increase" in the country's nuclear arsenal, signaling a continued flurry of military activities in the new year. Yoon also warned this week that he would consider suspending a 2018 inter-Korean military agreement if the North violates the South's territory again. The pact, part of former liberal president Moon Jae-in's efforts at rapprochement with Pyongyang, consists of measures such as setting up buffer zones, ceasing loudspeaker propaganda and demining the heavily armed inter-Korean border. During his election campaign, Yoon denounced his predecessor's "subservient" attitude toward Pyongyang and promised a tougher stance, even as he offered economic incentives for the North to ditch its nuclear program. Since Yoon became president in May, Seoul has resumed large-scale drills with its closest ally, the United States, to deter North Korea.
Return to Top	

HEADLINE	**01/05 Students in Iran rise up against government**
SOURCE	**https://www.washingtonpost.com/world/2023/01/05/iran-protests-students-mahsa-amini/**
GIST	Universities have been the beating heart of Iran's anti-government uprising, but the cost for students protesting in the Islamic Republic has never been higher, according to current and former activists. "They are getting killed, arrested, banned from campus, long prison sentences," said Nasim Sarabandi, a former student leader of the 2009 Green Movement protests for electoral reform, who fled Iran more than a decade ago to escape persecution. "I once thought it was too much to handle, what happened to me. But look at what [authorities] are doing … years later, how much of an expense the students are paying, what a sacrifice they are making." The price paid by this generation of Iranian students demanding their rights is rising day by day. And as the repression deepens, they are giving up on the fight for reform — for years a rallying cry of student movements. The young men and women who have risked their lives and futures in demonstrations over the past several months want nothing less than the end of oppressive clerical rule. Campus actions have taken place nearly every day since mid-September, following the death of 22-year-

old Mahsa Amini in police custody after she was detained for an alleged clothing violation. Iran's clerical leaders, and the fearsome security services that back them, have responded with a wide-ranging crackdown. Security forces have killed more than 500 people and arrested some 19,000, according to the activist news agency HRANA. Two men have been executed in connection with the protests.

"The regime maximizes pressure on students to an extent that you cannot walk, dress, talk or even laugh in a way that doesn't match their standards," said a student activist with the Progressive Students of Isfahan union, founded in 2018 in defiance of Iran's ban on independent unionizing.

"We are well aware that as soon as protests stop, they'll go back to their maximum pressure again. … Our main purpose is to eliminate this system altogether," the student told The Washington Post. Like others interviewed for this story, he spoke on the condition of anonymity for fear of government reprisals.

HRANA has documented protests at 144 universities and, as of Wednesday, the Volunteer Committee to Follow Up on the Situation of Detainees had confirmed the arrest of 685 university students. At least 44 have been sentenced, often to multiple years in prison. More than half remain behind bars and at least one student faces charges that could merit the death penalty, the committee said.

The university activist in Isfahan, in central Iran, said his union has received continuous reports from across the country of plainclothes police kidnapping students on campus and of indiscriminate beatings by volunteer forces. Volleys of tear gas, sound bombs and pellet bullets fired at student protesters have caused skull fractures and eye injuries.

The Post could not independently confirm these accounts, but they are consistent with the findings of rights groups and U.N. experts.

An untold number of students arrested have faced abuse, torture or sexual assault in detention, the activist said. Others have been sentenced to months or years in prison in hastily held trials lacking due process, or banned from university dorms and campuses and barred from traveling abroad.

One fed-up woman in Tehran told The Post she quit school after being threatened by her university for boycotting classes in protest. She dreams of continuing her studies abroad, she said, but that will require paperwork now difficult to acquire. One man in Tehran, in between protests and coursework, said he is caring for a friend struggling to finish his thesis while battling suicidal thoughts that developed after authorities broke his arm in jail.

University students have long been agents of activism in Iran — during protests against press restrictions in 1999 and again during the Green Movement in 2009. Part of what's different this time, activists said, is that years of suppression leading up to the uprising pushed university organizing underground. While the regime's response has been comparatively quicker and more violent, there is no core student leadership to crush. The decentralized nature of the protests is central to their endurance.

"As much as the oppression has spread, the activism has spread," said Sarabandi, who was repeatedly jailed and threatened.

After the 1979 revolution, Iran banned student organizing outside of the state-backed Islamic student associations. For many years, however, some of these associations had lively debates, elected national boards and advocated for reform.

This changed after the 2009 presidential election when the reformist candidate Mir Hossein Mousavi, backed by student movements, lost to hard-line incumbent Mahmoud Ahmadinejad, who had the support of Iran's supreme leader and the Revolutionary Guard Corps. Mousavi was widely popular, and Ahmadinejad's win set off massive demonstrations, known as the Green Movement, against the allegedly rigged election.

The Tehran man, a 37-year-old completing a PhD in cognitive science, took part in the 2009 protests.

	Then pursuing his undergraduate degree, he attended seminars and rallies on campus, where he met other like-minded students. Basij police forces beat him during protests, he said, but he was never detained. These days "are much scarier," he said. He has been beaten and shot with pellet bullets in recent months and considers himself "lucky" to have avoided arrest. He says he is haunted by the image of a young woman being brutally beaten by security forces. He was helpless to stop them. Sarvenaz, 27, the female university student in Tehran, who is pursuing a master's degree in psychology, said she boycotted classes for weeks, but returned ahead of exams on Dec. 9, the day after the first execution tied to the uprising. "That day I felt very bad about myself, going back to the oppressive atmosphere at our university," she told The Post. She gritted her teeth through the security inspection at the entrance, where guards checked that women were veiled and that banned students didn't enter. In one class, a debate broke out over why she and others had been absent. "I went back home and cried the whole way," she said. "Then I realized that I can never be a student in Iran again because I cannot tolerate this level of oppression and pressure." She says she will keep protesting. Mehdi Arabshahi, another student leader in 2009 who was imprisoned several times and now lives in exile in Virginia, said he was "very worried about the students in prison now because the conditions are much harder, the sentences much longer." "They are very radical and they are very brave," he said. "When I was a student activist, the dominant paradigm was a kind of reform in Iran. But these days the dominant paradigm is a kind of revolution, or regime change."
Return to Top	

HEADLINE	**01/04 Winter warmth sets records eastern US**
SOURCE	**https://www.washingtonpost.com/weather/2023/01/04/record-warm-weather-eastern-united-states/**
GIST	Less than two weeks removed from a Christmastime Arctic blast for the ages, much of the eastern United States has been bathing in record warmth to kick off January. This warm spell gathered steam to begin the new year before intensifying and expanding eastward. Both Monday and Tuesday featured several dozen high temperature records, from the South and Gulf Coast to the Midwest and Northeast. It's the second pulse of springlike warmth during the past week. The first delivered numerous records to the Northeast and Florida over the weekend. The current warm spell peaked Wednesday morning, with low temperatures at least 20 to 30 degrees above normal from Alabama to Michigan, extending east into the Mid-Atlantic. These low temperatures were close to the warmest on record for about 100 locations. While some locations just missed records, many posted their warmest Jan. 4 lows; a few even saw lows at or near record-warm levels for the entire month of January. Here is a partial list of the Jan. 4 record-warm lows (assuming these temperatures do not fall before midnight): • Key West, Fla. — 77 degrees, topping 76 in 2019. This is two degrees from the monthly record. • Norfolk — 64 degrees, topping 62 in 2004. This also marked the warmest low for the entire month. • Raleigh, N.C. — 62 degrees, topping 58 in 1950. • Salisbury, Md. — 62 degrees, topping 60 degrees in 1950. This is one degree from the monthly record. • Morgantown, W.Va. — 58 degrees, topping 56 in 1997. • Atlantic City — 54 degrees, topping 52 in 1950. This is one degree from the monthly record.

- New York Central Park — 57 degrees, tying 1950.
- Dulles, Va. — 55 degrees, topping 51 in 1997.

High temperature ranking on the warm side for Jan. 3. (Southeast Regional Climate Center)
In addition to these record warm lows, many record highs were set Tuesday from the Ohio Valley to the Mid-Atlantic, including in:

- Tallahassee — 85 degrees, topping 80 in 2017.
- Beaumont-Port Arthur, Tex. — 82 degrees, topping 81 in 1989.
- Huntsville, Ala. — 81 degrees, a record for Jan. 3 and for the entire month.
- Knoxville, Tenn. — 75 degrees, topping 74 in 2000.
- St. Louis — 72 degrees, topping 68 in 1939.
- Washington — 69 degrees, topping 68 in 1950.
- Mansfield, Ohio — 61 degrees, topping 59 in 2004.

Washington has hit at least 60 degrees on each of the first four days of January, for the first time on record.

This surge of winter warmth commenced Monday, with a focus on the South. A select list of Monday's record highs includes:

- Austin — 83 degrees, topping 80 in 1954.
- Mobile, Ala. — 82 degrees, topping 80 in 2006.
- Fort Smith, Ark. — 77 degrees, topping 75 in 2004.
- Atlanta — 74 degrees, topping 73 in 2022.
- Chattanooga, Tenn. — 70 degrees, topping 69 in 1952.
- Charlottesville — 69 degrees, topping 65 in 2022.

The warmth in the East is a response to the stormy weather in California. The jet stream is taking a dip in the western United States, helping to bring precipitation systems ashore. Like a seesaw, when one part of the jet stream dips, the other side bulges northward, carrying warm air along with it.

The record temperatures in the eastern United States follow an exceptional burst of warmth in Europe that began on New Year's Eve and has yet to fully relent. Leeming in central Britain matched its warmest January low on record Wednesday. That record was among thousands set in Europe since Saturday.

The concurrent warm spells in Europe and the eastern United States are further examples of how human-caused climate change is increasing the frequency of abnormally high temperatures. Although the pre-Christmas Arctic blast in the United States set record lows, the cold was not sustained, and statistics make clear that extreme warmth has become much more common.

Return to Top

HEADLINE	**01/04 Ohio bans 'gas station heroin'**
SOURCE	**https://www.vice.com/en/article/g5ve9q/ohio-bans-zaza-tianeptine**
GIST	Ohio just became the latest state to ban tianeptine, an antidepressant known as "gas station heroin" because it can mimic the effects of opioids and is being sold at gas stations, convenience stores, and online. Republican Gov. Mike DeWine signed an executive order allowing the state's Board of Pharmacy to issue an emergency ban on tianeptine products on Dec. 22, according to a news release, which cited reporting from VICE News. The ban means tianeptine products, which are often marketed as dietary supplements under names like ZaZa, Tianna, TD Red, and Pegasus, are now considered a Schedule I drug in the state and are illegal to sell. Vendors and consumers who violate the ban are subject to penalties that range from mandated drug treatment, fines, or 6 to 12 months of jail time. The Board of Pharmacy found that tianeptine has "no accepted medical use in treatment in this state and

	poses an imminent hazard to the public health, safety, or welfare." Michigan, Alabama, Minnesota, Tennessee, Georgia, and Indiana have also banned tianeptine, and in February, the FDA issued a warning stating that it's been associated with "serious harm, overdoses, and death." Tianeptine is a tricyclic antidepressant available via prescription in some countries in Europe, Latin America, and Asia, but it's not approved for use in the U.S. Experts previously told VICE News there's little transparency as to exactly how much of it—and other chemicals—are in the products being sold in gas stations. Because tianeptine hits opioid receptors in the brain, it can mimic opioid toxicity and withdrawal. Some users told VICE News they're hooked on it and have experienced intense withdrawals when they've stopped using it, even after a few hours, with symptoms that include severe anxiety, restlessness, nausea, vomiting, and chills. "We're certainly hoping folks will just say 'Hey this is garbage… we should get rid of it'," said Cameron McNamee, a spokesman for the Ohio Board of Pharmacy. McNamee said the state has alerted local public health departments and police departments about the ban and is planning on sending out more notices translated into different languages to help spread awareness. "The availability of an unregulated, tricyclic antidepressant without any medical supervision presents a serious risk to public health. Media reports indicate that patients are utilizing tianeptine to either manage withdrawal or initiating use based upon the reported opioid-like effects," the news release said, referencing a VICE News story.
Return to Top	

HEADLINE	**01/04 Pentagon to bolster Guam's defenses**
SOURCE	**https://www.washingtontimes.com/news/2023/jan/4/inside-ring-new-missiles-radars-bolster-guam-defen/**
GIST	The Pentagon is moving ahead with new radar systems in the South Pacific in response to the growing threat of Chinese missile strikes against the major U.S. military hub on the Pacific island of Guam. The Pentagon announced a contract award last month for a new tactical over-the-horizon radar system to be built on the island nation of the Republic of Palau. The Navy contract announced Dec. 28 is for $118 million to build reinforced concrete pads and foundations for the radar and will be done by the California-based construction company Gilbane Federal. The same day, Lockheed Martin won a contract from the Pentagon's Missile Defense Agency for $527.7 million to expand missile defenses on Guam with what the Pentagon is calling the Aegis Guam System. The defense buildup on Guam comes as a Chinese aircraft carrier recently sailed near the U.S. island territory. The Liaoning and several other warships conducted exercises near Guam that included an estimated 260 aircraft sorties in the region, according to defense sources. The warships were near Guam from Dec. 17 to Dec. 27 and were closely monitored by U.S. military assets in the region. The highly effective Aegis missile defense system has been deployed on Aegis warships for years. The system on Guam will be the ground-based version known as Aegis Ashore, which will be powered by an advanced phased-array radar system called SPY-7 that can monitor air and space in all directions. The missile interceptors will be SM-3s, which can be used against ballistic missiles, and possibly SM-6s to target cruise missiles. The target date for completion of the Guam Aegis System is 2027. The Missile Defense Agency announced in March that it plans to spend nearly $900 million to upgrade Guam's defenses, including the Aegis system and the Army's Terminal High Altitude Area Defense

	(THAAD) system, which is currently deployed on Guam along with a temporary deployment of the Israeli-made Iron Dome defense system. Patriot missile defenses will also be added to provide a "layered" defense against aircraft and missiles. China has deployed a new intermediate-range missile, the DF-26, that state media has called a "Guam killer" because it can strike targets on the U.S. island. A report by the National Institute for Public Policy said the road-mobile DF-26 "is China's first precision strike capability with both conventional and lower-yield nuclear variants capable of striking Guam." U.S. military assets at the Guam hub are projected to take a major role in any future defense of Taiwan against an attack from the mainland. U.S. Indo-Pacific Command war planners anticipate that a conflict with China over Taiwan will involve Chinese missile strikes on Guam, which hosts U.S. bombers such as the B-52, B-2 and B-1. Recent satellite photos published by EurAsian Times revealed that China is practicing missile strikes in the Xinjiang desert using targets built in the shape of Guam, with targets that included mock-ups of U.S. aircraft carriers and destroyers. Beijing posted online in 2020 a military video showing a simulated attack on Andersen Air Force Base, Guam. Palau, which is about 800 miles from Guam, is used for military exercises, including a recent Patriot missile defense exercise. The tactical mobile over-the-horizon radar system, known as TACMOR, is expected to greatly boost surveillance of the region for the U.S. military. The high-technology radar uses advanced computer capabilities to extend radar coverage thousands of miles beyond conventional radar. Along with TACMOR, the Navy is building communications infrastructure to transmit the radar's data to a remote operations center that will then send the data to U.S. and allied military forces in real time. The installation is slated for completion by 2026. Congress has pressed the Pentagon to bolster defenses on Guam, and the recently passed defense authorization bill for fiscal 2023 mandated building an integrated air and missile defense system for the island.
Return to Top	

HEADLINE	**01/04 World's first vaccine for honeybees**
SOURCE	**https://www.theguardian.com/environment/2023/jan/04/honeybee-vaccine-first-approved**
GIST	The world's first vaccine for honeybees has been approved for use by the US government, raising hopes of a new weapon against diseases that routinely ravage colonies that are relied upon for food pollination. The US Department of Agriculture (USDA) has granted a conditional license for a vaccine created by Dalan Animal Health, a US biotech company, to help protect honeybees from American foulbrood disease. "Our vaccine is a breakthrough in protecting honeybees," said Annette Kleiser, chief executive of Dalan Animal Health. "We are ready to change how we care for insects, impacting food production on a global scale." The vaccine, which will initially be available to commercial beekeepers, aims to curb foulbrood, a serious disease caused by the bacterium Paenibacillus larvae that can weaken and kill hives. There is currently no cure for the disease, which in parts of the US has been found in a quarter of hives, requiring beekeepers to destroy and burn any infected colonies and administer antibiotics to prevent

	further spread. "It's something that beekeepers can easily recognize because it reduces the larvae to this brown goo that has a rancid stink to it," said Keith Delaplane, an entomologist at the University of Georgia, which has partnered with Dalan for the vaccine's development. The vaccine works by incorporating some of the bacteria into the royal jelly fed by worker bees to the queen, which then ingests it and gains some of the vaccine in the ovaries. The developing bee larvae then have immunity to foulbrood as they hatch, with studies by Dalan suggesting this will reduce death rates from the disease. "In a perfect scenario, the queens could be fed a cocktail within a queen candy – the soft, pasty sugar that queen bees eat while in transit," Delaplane said. "Queen breeders could advertise 'fully vaccinated queens.'" American foulbrood originated in the US, and has since spread around the world. Dalan said the breakthrough could be used to find vaccines for other bee-related diseases, such as the European version of foulbrood. As they have been commercialized, transported and pressed into agricultural service, honeybees have been exposed to a cocktail of different diseases that typically lay waste to large numbers of colonies and require major interventions by beekeepers to keep numbers up. The US is unusually dependent upon managed honeybee colonies to prop up its food pollination, with hives routinely trucked across the country to propagate everything from almonds to blueberries. This is because many wild bee species are in alarming decline, due to habitat loss, pesticide use and the climate crisis, fueling concerns around a global crisis in insect numbers that threatens ecosystems and human food security and health.
Return to Top	

HEADLINE	**01/05 Day 316 of the Russia invasion**
SOURCE	**https://www.theguardian.com/world/2023/jan/05/russia-ukraine-war-at-a-glance-what-we-know-on-day-316-of-the-invasion**
GIST	• **US President Joe Biden said that the US was considering sending Bradley Fighting Vehicles to Ukraine.** The armoured vehicle with a powerful gun has been used as a staple by the US army to carry troops around battlefields since the mid-1980s. • **The US is also looking at ways to target Iranian drone production through sanctions and export controls,** the White House said. Washington previously imposed sanctions on companies and people it accused of producing or transferring Iranian drones that Russia has used against Ukraine. • **Russia's defence ministry on Wednesday blamed the illegal use of mobile phones by its soldiers for a deadly Ukrainian missile strike that it said killed 89 servicemen,** raising the reported death toll significantly. Moscow previously said 63 Russian soldiers were killed in the weekend strike on Makiivka. Although an official investigation has been launched, the main reason for the attack was clearly the illegal mass use of mobile phones by servicemen, the ministry said. "This factor allowed the enemy to track and determine the coordinates of the soldiers' location for a missile strike," it said in a statement issued just after 1:00am in Moscow on Wednesday. • **The UK Ministry of Defence said that it was a "realistic possibility" that ammunition was being stored near troop accommodation in Makiivka:** "Given the extent of the damage, there is a realistic possibility that ammunition was being stored near to troop accommodation, which detonated during the strike creating secondary explosions," the UK MoD said in its daily intelligence briefing. "The Russian military has a record of unsafe ammunition storage from well before the current war, but this incident highlights how unprofessional practices contribute to

Russia's high casualty rate."

- **Heavy fighting around the largely ruined, Ukrainian-held city of Bakhmut is likely to persist for the foreseeable future,** with the outcome uncertain as Russians have made incremental progress, according to a senior US administration official.
- **The Ukrainian deputy defence minister said significant Russian losses meant Moscow would probably have to announce a second partial mobilisation** in the first quarter of the year.
- **Further strikes deep in Russian territory should be expected, the head of the Ukrainian military intelligence, Kyrylo Budanov, has told the US TV network ABC.** He added that the attacks would come "deeper and deeper" inside Russia, without specifically saying whether Ukraine would be behind them.
- **The French president, Emmanuel Macron said France would send light AMX-10 RC armoured combat vehicles,** an Elysee official said after a phone call between Macron and his Ukrainian counterpart, Volodymyr Zelenskiy.
- **Ukraine's military general staff said Russia had launched seven missile strikes, 18 airstrikes and more than 85 attacks from multiple-launch rocket systems in the past 24 hours** on civilian infrastructure in three cities – Kramatorsk, Zaporizhzhia and Kherson. "There are casualties among the civilian population," it said. The reports have not been independently verified.
- **Ukraine's efforts to increase exports under the Black Sea grain deal with Russia are focused on securing faster inspections of ships** rather than including more ports in the initiative, a senior Ukrainian official said on Wednesday.
- **Ukraine's navy has claimed Russia has three combat-ready ships in action in the Black Sea** and that it continues to "violate the international convention for the protection of human life at sea 1974 (Solas), disabling auto identification systems on civilian vessels in the Azov Sea", it said in a post on Facebook.
- **Vladimir Putin took part in a ceremony by video link while the Russian frigate Admiral Gorshkov went into combat service equipped with the Zircon hypersonic missile systems.** The Russian president said: "I am sure that such powerful weapons will reliably protect Russia from potential external threats and will help ensure the national interests of our country". The defence minister, Sergei Shoigu, said the Gorshkov would sail to the Atlantic and Indian oceans and to the Mediterranean Sea.

Return to Top

HEADLINE	**01/04 Auto sales drop to worst level in decade**
SOURCE	**https://www.wsj.com/articles/auto-industry-expected-to-post-worst-u-s-sales-year-in-more-than-decade-11672808763?mod=hp_lead_pos6**
GIST	The U.S. auto industry posted its worst sales year in more than a decade in 2022 as supply-chain snarls and poorly stocked dealerships dented results for many car companies. With few exceptions, auto makers on Wednesday reported sales declines for the year. General Motors Co. was one of the few to report an increase, after recovering from factory shutdowns that were caused by parts shortages. The Detroit auto maker retook its U.S. sales crown from Toyota Motor Corp. after losing the top spot in 2021 for the first time in decades, an upending of the traditional pecking order that largely occurred because of supply constraints. Industrywide, U.S. auto sales totaled 13.7 million vehicles in 2022, the lowest figure since 2011 and an 8% decrease from the prior year, according to the research firm Wards Intelligence. Sales had topped 17 million vehicles for five straight years before the Covid-19 pandemic struck in 2020, unleashing supply-chain problems that have bogged down deliveries ever since. Several car executives said they were encouraged by relatively strong sales in the fourth quarter as factory work accelerated in the midst of improved parts supply. Now, though, some worry that the supply problems of the past few years could morph into a demand problem, with rising interest rates and

inflationary pressures weighing on consumers' ability to afford new wheels.

"It's going to make things a lot more challenging in 2023," Hyundai U.S. chief Randy Parker said, referring to rising rates, after his company posted a slight sales decline for 2022. "There's still a lot of pent up demand."

The drop in 2022 vehicle sales marks a reversal for a sector that started the year hoping historically low interest rates and an end to parts shortages would fuel a rebound in sales. Instead, vehicles continued to be in short supply as car makers mostly waited for scarce computer chips. Russia's invasion of Ukraine, a key supplier of auto parts, added to the supply-chain troubles.

"When we started the year off, the whole industry had projections all above 16 million," said Jack Hollis, Toyota's North American sales chief. Companies quickly ditched their projections as factories were forced to shut down or slow production.

"It's not all doom and gloom," Mr. Hollis said. There are early signs that the shortages and rising raw-material prices are easing. Many car makers reported an improvement in their sales near the end of the year as computer-chip supplies began to improve. Mr. Hollis said Toyota expected the industry to sell 15 million vehicles this year.

Nissan Motor Co.'s U.S. sales fell by about 25% in 2022, but declined only 2% in the fourth quarter in the midst of enhanced semiconductor availability. "It's definitely improved," said Judy Wheeler, who oversees U.S. sales for Nissan. "I'm hoping it won't be an issue as we move forward."

A prolonged shortage of semiconductors created pent-up demand for new vehicles, which meant that cars and trucks went to waiting buyers almost as soon as they hit the dealer lot. The lack of availability left buyers paying top dollar for the rides they could secure, pushing the average price paid for a vehicle in December to a near record high of $46,382, according to J.D. Power.

The strong pricing buoyed auto-maker profits last year despite shrinking sales volume and insulated the industry from a broader decline in consumer spending.

Some analysts caution that it is still too early to tell whether rising prices are pushing buyers away. Heavy snowfall in large parts of the northern U.S. weighed on December sales, making it hard to see the impact of higher prices, JPMorgan analysts wrote in a note to clients.

Still, there are early signs that demand might be slowing, even for the hottest car makers.

Tesla Inc. reported Monday that it fell short of its growth projections last year, in part because of Covid-related shutdowns at its Shanghai factory and changes in the way it manufactures and distributes vehicles.

Analysts have pointed to decreased wait times for Tesla vehicles as a sign of softening demand. Tesla offered a rare discount on some of its vehicles if buyers agreed to take delivery before the end of 2022.

Electric-vehicle sales accounted for nearly 6% of the retail market in the U.S. in 2022, up from about 3% in the prior year, according to J.D. Power.

Executives have been investing billions of dollars on new models and factories, in the belief that sales will continue to expand rapidly over the next decade.

But rising prices for raw materials used in lithium-ion batteries pushed up electric-vehicle prices throughout 2022, and some executives warned of a looming battery shortage.

GM cut its electric-vehicle sales target for 2023 because of a slower-than-expected increase of battery production.

	The semiconductor shortage, while easing for some other sectors, such as smartphones and personal computers, remains a challenge for autos, in part because car companies typically use inexpensive, commodity silicon for vehicles. Toyota, citing a lack of chips, cut its production outlook for the current fiscal year through March. Declining used-car prices are driving down the value of trade-ins, a development that is discouraging to potential buyers who intend to use the equity in their existing vehicles to offset the higher cost of purchasing a new one. That bodes poorly for sales this year, as retailers worry that buyers who were unable to buy a car as a result of shortages will now be priced out of the market, according to a survey of dealers conducted by Cox Automotive. The research website Edmunds expects new-car sales to hit 14.8 million in 2023, a marginal increase from last year but well below prepandemic levels. A combination of rising rates, inflation and economic turmoil could push vehicles out of reach for many buyers, Edmunds said.
Return to Top	

HEADLINE	**01/04 Ukraine postal workers lead reintegration**
SOURCE	**https://www.wsj.com/articles/ukraines-postal-workers-lead-the-way-in-reintegrating-reclaimed-lands-11672830890?mod=hp_lead_pos7**
GIST	DARYIVKA, Ukraine—Standing behind her post office counter with bricks of cash, a calculator and a flashlight, Lyudmila Gulovskaya distributes Ukrainian state pensions to a line of eager onlookers in this front-line village near Kherson. For these pensioners, it is the first money they have received from Kyiv in six months, after their villages in surrounding areas were occupied by Russian soldiers. For Ms. Gulovskaya, it is the most tangible proof yet that their government has returned. “We’re back in business,” she said, with the sound of artillery in the distance. “People are poor here; they wouldn’t survive here without the post office.” After Kyiv’s forces take back a front-line village or town and continue onward, the job of reintegrating it back into the map of Ukraine begins. And in a country where the post office is responsible for distributing pensions to the elderly and letters haven’t been entirely replaced by email, that delicate task largely falls to Ukraine’s postal service, or Ukrposhta. “When Ukraine takes back territory, first the military goes in, then the de-miners go in, then we go in,” said the chief executive of the postal service, Igor Smelyansky. “We’re the first symbols of Ukraine they see.” Not only is Ukrposhta responsible for the first injection of cash meant to jumpstart the local economy after months of erratic price rises on products brought in from Russia, Mr. Smelyansky has also distributed generators and Starlink communication systems to branch offices around the country to turn them into shelters, offering heat, electricity and internet in areas where fighting has crushed critical infrastructure. “For people who have lost everything, trust is everything,” he said. For years, Russia has dismissed the strength of Ukraine’s state institutions, pointing to the country’s rampant corruption. But in the face of Moscow’s invasion, employees at all levels in Ukraine’s state companies have kept the economy running and become the engines of reintegrating Ukraine’s once-occupied lands. When Russian troops first arrived in Darivka, in the Kherson region, and other occupied towns and cities, their first task was to convince residents that Ukraine had abandoned them and that Russia was there to stay. They took down Ukrainian state symbols and flags and put up billboards celebrating Russian culture

and Ukraine's domination.

For Ukrainians, the post office is an essential and familiar part of life, and Russians' attempt to take it over laid the groundwork to legitimize Moscow's own claim to the region. Those moves worked to buttress Russian President Vladimir Putin's own assertion that the country had been artificially created and never had a "tradition of genuine statehood."

The Russians let the post office continue to run, distributing cash to keep residents happy until mid-summer, when they tried to end the use of the Ukrainian hryvnia and replace it with the Russian ruble. Mr. Smelyansky tried keeping hryvnias flowing to regions behind the front line, bringing them in boxes through military checkpoints or getting local companies to pay out hryvnias to pensioners while depositing cash in their accounts from Kyiv.

But by June, it had become too hard, and Ukrposhta said it was stopping operations in the Kherson region. When postal employees gathered on June 30 in the top regional office to hear about the future of Ukrposhta there, Russian soldiers burst in and local collaborators said they were taking over the offices, said Olga Yeshchenko, 47, the head of the branch's human-resources department.

"They hijacked the moment to get people to join them," she said.

The next day, Ms. Yeshchenko sent Mr. Smelyansky resignation notifications from employees who refused to work with the Russian authorities, though some stayed behind. She sent her own resignation and days later left the western region of Ternopil.

As the Russians took over, they seized property, too. The director of the Kherson post office, who had joined the Russians, told employees who were trying to hide records and computers that they would be "thrown in the basement" if they didn't hand over the equipment.

While the Kherson post office building was used for little more than handing out one-time pensions of about 10,000 rubles, about $160, occupation authorities elsewhere tried to develop their own postal services.

When Mr. Smelyansky visited his newly de-occupied postal branch in the eastern Donbas area city of Lyman, he found a newly made storefront sign still in wrapping for the Donbass Post, using the Russian spelling for the region. He said Russia was slowly trying to integrate the small postal offices into its federal system.

But even with the Russians gone, some sympathies for Moscow still remain, particularly in Ukraine's east.

"Some people out there aren't big fans of Ukraine, so it's a challenge," said Mr. Smelyansky, who traveled on Christmas Eve to the village of Nevsky in the Donbas region of Luhansk to dispense pensions to villagers for the first time in five months.

While Ukraine has had a Ministry of Reintegration since Russian-backed forces set up statelets in the country's east in 2014, its offices have been more focused on distributing humanitarian aid. That has left the process of reconciliation between those who supported the opposing sides of Moscow and Kyiv to people on the ground.

"I wish we could do more," said Mr. Smelyansky, a former U.S.-based consultant who was brought in to run Ukrposhta in 2016, when the loan terms from the International Monetary Fund demanded independent heads be recruited to run state companies.

The reopening of Ukrposhta branches in some of Ukraine's farthest-flung regions that were under Russian occupation has presented the problem of finding new employees who can be trusted.

	Those who worked under Russian authorities have been banned. New hires have a monthlong probation period, during which Ukraine's domestic intelligence agency, the Security Service of Ukraine, investigates their history during the occupation, searching for collaborators or those with pro-Russian sympathies. "We're trying to build Ukrposhta back up as fast as we can, but there are challenges," said Tatiana Morozova, the head of the company's operations in the Kherson region. "But we've taken a decision not to hire collaborators, and we're sticking by it." In the center of Kyiv, the Ukrainian postal service's cavernous warehouse holds the bulk of packages waiting to be delivered to the far reaches of Ukraine under Russian occupation. Every time Kyiv's forces take back a new village or city, a few more dozen packages are shipped out—and delivered. Still, around 300 packages are waiting to be delivered to occupied areas of Ukraine, including Mariupol, which Russian troops took in May following a monthslong bloody siege, Mr. Smelyansky said. About $300 million is also waiting to be dispensed to pensioners in those areas, he added. Earlier this month, Yelena Ryabchenko, 63, was standing in line in the central Kherson post office to dispatch the first package she has been able to send to her son in prison in central Ukraine since the occupation began at the start of the invasion. She said it contained bread and fruit, but not a letter. Letters aren't allowed, she said. "We're part of Ukraine again," she said, her voice trembling. "I never thought much about it before, but if I can send packages to my son, that's all that matters." In the village of Daryivka, inside the makeshift postal offices, Olha Yaroshchenko, 65, stepped aside from the counter where she had just received 16,800 hryvnia from Ms. Gulovskaya to count the cash a second time. "All I need to buy right now is firewood and coal," she said. "It's been six months without my pension and it's cold outside."
Return to Top	

HEADLINE	**01/04 Australia to deploy US HIMARS**
SOURCE	**https://www.wsj.com/articles/australia-to-deploy-u-s-himars-rocket-system-being-used-in-ukraine-11672892032?mod=lead_feature_below_a_pos1**
GIST	SYDNEY—Australia said it will acquire a highly mobile, U.S.-built rocket system that can strike targets from far behind the front lines, the latest step by the U.S. ally to beef up its military amid increased competition with China in the region. The system, the High Mobility Artillery Rocket System, or Himars, has gained prominence after being used effectively by Ukrainian forces against Russia. The system involves trucks that can carry satellite-guided rockets and strike targets up to about 185 miles away with high precision. Ukrainian troops used Himars provided by the U.S. over the summer to halt a Russian advance and have hit Russian ammunition depots, logistics supplies and command centers. The rocket system can do a job that previously needed dozens of launchers firing thousands of shells, allowing an armed force to be light and mobile and helping to revolutionize modern warfare. "In the current strategic environment, it's important the Australian Defence Force is equipped with high-end, targeted military capabilities," said Richard Marles, Australia's defense minister. Australia said that the Himars will include a weapon-locating radar to detect and respond to land, air and sea threats, that its range could increase with technological advances, and that the system will be in use as early as 2026. Australia didn't publicly say how many Himars it would purchase, but U.S. officials last year approved the sale of 20 Himars and related equipment to Australia, for an estimated $385 million,

from contractors including Lockheed Martin Corp.

"Australia is one of our most important allies in the Western Pacific," the U.S. Defense Security Cooperation Agency said last year. "It is vital to the U.S. national interest to assist our ally in developing and maintaining a strong and ready self-defense capability."

The sale is another sign of the deepening defense cooperation between the U.S. and Australia, which have grown closer in recent years as concerns rise about a possible conflict with China. China says its foreign policy aims for peace, but Beijing has pledged to take control of Taiwan by force and some Western officials fear it could invade in the coming years.

Last month, the U.S. said it would deploy more military assets in Australia, highlighting Australia's central role to U.S. strategy in the region. Officials said then that the two countries would jointly develop airfields in northern Australia, which could be an important staging ground for allied forces in any future conflict in the region and where U.S. Marines have already been training.

The two countries have also signed a three-way military pact with the U.K. that will help Australia develop a nuclear-powered-submarine capability. Australia has also previously said it wanted to build guided weapons domestically and boost the overall size of its military.

The Himars system will help Australia to enhance its long-range strike capability, which strategists say provides crucial deterrence and has been a focus of Australian military planners. A 2020 strategic update from Australia's defense department said the military would invest in longer-range strike weapons to hold off potential adversaries farther from the country's shores.

Still, some military analysts have raised concerns about a broader capability gap for Australia's long-range strike abilities given that a fleet of nuclear-powered submarines, which have extensive range and speed, isn't expected to be in place for many years. Analysts expect a review of Australia's military, announced in August last year and anticipated to be released in the coming months, to tackle that issue.

Possible ways Australia can further boost its long-range capabilities include acquiring the new B-21 stealth bomber, developing new hypersonic long-range missiles, drones or even a new concept that involves using military cargo aircraft to drop munitions, analysts at the government-backed Australian Strategic Policy Institute said in a report last month.

The worst-case scenario for Australian military planners is the possibility that an adversary establishes a presence near Australian shores and either targets the country or cuts it off from allies such as the U.S., the report said. It warned that China's ability to project force has grown in the past two decades and that it includes long-range conventional ballistic missiles, bombers and ships.

Separately, Australia said it had signed a contract with Norwegian company Kongsberg for a new naval strike missile that will be deployed on Australian destroyers and frigates. That missile will replace an aging antiship missile.

"The level of technology involved in these acquisitions takes our forces to the cutting edge of modern military hardware," said Pat Conroy, Australia's minister for defense industry.

Return to Top

HEADLINE	**01/04 China throttled anti-Covid protests**
SOURCE	**https://www.washingtonpost.com/world/2023/01/04/china-surveillance-protests-security/**
GIST	China's rapid reversal of strict "zero covid" policies following unprecedented protests in November appeared, from afar, to be a rare instance of authorities acknowledging — perhaps even tacitly condoning — popular public dissent. But as Beijing loosened its iron grip on the coronavirus, a different story was unfolding inside homes and

police stations across the country as authorities fanned out to crack down on those behind the protests — utilizing the powerful surveillance state built over the past decade and fine-tuned during the pandemic.

Dozens of people who took part in the protests have paid heavily for the dissent, subject to intense surveillance measures and aggressive interrogations in police custody, even as Beijing was shifting to unravel the policies.

Protesters in Beijing and Shanghai describe heightened digital surveillance, strip searches, threats against their families, and being forced into physical duress during interrogation.

The stories give fresh insight into the mechanisms put in place by Beijing to quash criticism of the government. They also highlight the perilous line regular people walk in expressing dissent in China — where opaque systems of policing and high-tech surveillance make protests rare and brief, while manipulation of the legal system and online debate often lead to ruinous repercussions.

“The virus is no longer the enemy, the health officials and quarantine are not the enemy … now only the people who protest are the enemy,” said Doa, a 28-year-old tech worker in Beijing who was detained after a protest. People who spoke to The Washington Post about interactions with police offered nicknames or spoke on the condition of anonymity because of the sensitivity of the matter.

Doa and a friend were at a protest near the Liangmahe bridge in eastern Beijing for around half an hour just after midnight Nov. 28 and kept a low profile, steering away from those filming on their cellphones and avoiding direct interactions with police. “I worked before in the social media industry. … I know how those things can be used by police,” she said. “They still found me. I’m still wondering how that is possible.”

Two days later, she awoke to a string of frantic calls and text messages from her mother, who said that police had called to tell her that her daughter had participated in “illegal riots” and would soon be detained. “I don’t know why they did it that way. I think it creates fear,” Doa said.

A few hours later, the police called her directly. She was summoned to a police station in northern Beijing, where her phone was confiscated and she underwent a series of interrogations over roughly nine hours.

“I had to undress to my underwear for a short period, it was very uncomfortable. They did not want to let me use the bathroom, for example.”

Doa said the police asked how she had heard about the protests, pushing for details of the accounts and names of people in her friend group.

“They wanted to know how I found out that the people were gathering. In the same way, I wanted to know how they knew about me, but I didn’t feel brave enough to ask. … I am not a political type person, I don’t write those things online,” she said. “All I can think of is that they knew my phone’s location.”

In the days and weeks following the unrest, authorities fanned out to find its instigators, setting into motion a police-led information-gathering network that has been fortified under President Xi Jinping with the aid of big data and high-tech policing.

There is no official figure on the number of people detained following the protests, and the Chinese government has not directly acknowledged arrests even occurred.

The Central Political and Legal Affairs Commission, which oversees domestic law enforcement, issued a non-specific warning that there would be a “crackdown” on any “infiltration and sabotage activities by hostile forces.” When a Foreign Ministry spokesman was asked about the arrest of protesters in November, he said only that reports did not reflect reality. But accounts from protesters and lawyers suggest there were at least dozens of similar incidents.

The Washington Post could not independently verify the accounts of the protesters. Two police stations in Beijing where incidents described by detainees occurred could not be reached for comment. Staff from a third police station in Shanghai declined to comment when reached by phone.

A web of silent surveillance

It's not clear exactly how police traced protesters such as Doa in the vicinity of the November protests, but insights from lawyers, analysts, protesters and police purchasing documents offer some hints at the types of tools used.

Among protesters and human rights lawyers, one leading theory — considered likely but difficult to prove — is that the police used cell signal towers to pull all phone numbers from locations where crowds gathered and then deployed officers en masse to work through the list.

"[The police] seem to have used some modern technology, network technology, and they have collected a data pool of phone numbers of all the people involved in the incident," said one lawyer with direct knowledge of protester cases. Like other lawyers The Post spoke to, they spoke on the condition of anonymity because of the matter's sensitivity.

"People have been called in for questioning one after another," they said.

Since Xi came to power 10 years ago, China has undergone a revolution in the way it polices dissent, eroding anonymity online and in the real world by embracing widespread data collection and automated surveillance tools.

The government has also rapidly expanded the legal obligations of internet companies to share information with authorities, requiring them to not only provide information in criminal cases but also detailed data on broader threats to the Communist Party.

It includes a 2018 policy requiring internet companies to make regular detailed reports on trends that "mobilize" public sentiment or cause "major changes in public opinion." Under the rule, companies must provide detailed information on individual users, including their real name, location and chat logs.

At the same time, China has blanketed its cities with hundreds of millions of surveillance cameras under an ambitious 2016 program called Sharp Eyes that set a goal of covering the entire population by 2020. It includes facial recognition cameras designed to automatically identify pedestrians and drivers and compare them against national ID registries and blacklists.

Police procurement documents issued in the years and months leading up to and immediately after November's protests shed light on how these technologies were used during them.

They include advanced facial recognition cameras designed to raise alarms when "abnormal" crowd behavior is detected and track people across different locations over an extended period. They also include technology used to scrape and analyze cellphone data from hundreds of domestic and foreign apps.

In Beijing's Chaoyang district, where Doa and other protesters gathered at the Liangmahe bridge, a 2018 police purchasing document describes "100% [surveillance] coverage," using more than 19,200 advanced cameras. The documents, which have not been previously reported, are made public inside China but not easily accessible.

The purchase order notes facial recognition cameras in the system must be able to immediately log a pedestrian's "name, former name, organization, gender, age, ethnicity, including whether they are Uyghur or not, and birth date," and maintain the logs for months or longer. The cameras must also be able to carry out identification on people wearing masks or sunglasses.

A similar system was purchased in Shanghai's Xuhui district, where protests erupted in late November, and has undergone continuous upgrades. Police submitted a purchase request in December to blanket a single street near the protest site with 620 surveillance cameras.

The Post reviewed dozens of police procurements for phone-scanning technology in the cities where major protests were held, including mobile terminals that can be used on the street. They list more than 1,000 apps that the equipment scrapes for data when a cellphone is scanned, including Facebook and Twitter, fitness and ride-sharing apps, and encrypted messaging services.

A 'knock on the door'

While eavesdropping and data-collection devices were silently ransacking protesters, inside police stations, authorities were using more traditional methods of gleaning information.

The Post spoke with six people arrested who say they experienced stressful and physically demanding interrogations.

"We were only allowed to stand and could not talk to each other. They didn't let us sleep, and if I did, they would knock on the door to wake me up," said one Shanghai man, 25, who spoke on the condition of anonymity for fear of further repercussions.

He told The Post he was arrested during the protests near Shanghai's Urumqi road, which in November became a mourning site for 10 people killed in an apartment fire in Xinjiang — a toll that some linked to covid controls. He said police sifted through his phone during questioning, asking about his friend groups.

The man said he saw others detained who were handcuffed and forced into a squatting position for around an hour after failing to comply. He said officers punished them in the station by making them do squat exercises and copy by hand pages of political documents from the 20th National Congress of the Chinese Communist Party.

"The purpose [of questioning] was to find out who planned it; they thought it was the separatists or foreign forces," he said. The officers taunted men in the group with long hair, calling them gay, he added. "They would also call us traitors and running dogs and tell us to get the hell out of China."

Days after the protests, Chen Wenqing, head of the Communist Party's top law enforcement decision-making body, urged vigilance against "sabotage by hostile forces" and "criminal acts that disrupt social order."

The accusations of foreign influence echo Beijing's line on pro-democracy protests in Hong Kong, which in recent years has compelled a broad expansion in the surveillance of overseas social media services, which are banned in China but can be accessed through VPN technology.

The Post earlier reported that hundreds of police stations and government bureaus across China purchased big data surveillance tools to automatically identify individuals at home and abroad behind critical trends in public opinion on foreign social media apps.

A month before the protests began in Beijing, the city's Ministry of Public Security issued a procurement for a 580,000-yuan ($84,000) data surveillance project combining human analysts and automated scraping tools to undertake 24-hour screening of domestic and overseas news and social media accounts discussing issues that could snowball into dissent in China.

"Especially news related to domestic people's livelihood and hot social issues," the document reads. It says the network should be capable of collecting, analyzing and reporting thousands of relevant pieces of information to police each day, and must have methods of recovering deleted social media posts. Services targeted include Twitter and Facebook.

Reports from lawyers and protesters also suggest Beijing police circumvented log-in protocols using domestic telecommunications firms to provide details of two-factor authentication messages sent to citizens' phones. Under Chinese law, telecommunications providers are required to comply with such requests.

	A 31-year-old man in Beijing told The Post he was interrogated and detained overnight Dec. 2 after reposting a video of protest scenes on Twitter and the domestic app WeChat, though he had not participated in person. “There was no sleep, no rest. … Up until the moment I was dismissed, they made me believe I was going to prison for a long time.” He said that the evening after his detention he received a two-factor authentication message from Twitter that he hadn’t requested. “Even two weeks after it happened again … it feels like a scene in some horror movie where someone is always watching, but I don’t know for sure.” One human rights lawyer working with protesters received notifications of two attempted log-ins on their Telegram messaging account on Dec 1. The effort failed, but whoever was trying to access the account — the lawyer suspects it was the police — was able to input a one-time log-in code correctly, according to screenshots of the incident shared with The Post. Intense pressure on legal professionals who offer counsel to protesters leaves those facing prison sentences with little hope of a fair trial. “It’s very sensitive — more sensitive than our previous cases related to human rights activists and political dissidents,” said another lawyer who had been offering services to detainees until warnings from authorities. “There is a nationwide attempt to prevent lawyers from even giving legal consultation to these protesters, not to mention personally representing them.” **If all else fails, blame foreign influence** The protesters have also now been increasingly vilified online. Censors appear to be allowing selective discussion of the demonstrations — so long as it is critical. As coronavirus cases spike across China, nationalist commentators now regularly blame deaths and overcrowded hospitals on tangfei, or reclining bandits — a pun on official warnings not to lie down and let the virus run rampant — who they claim compelled the sudden dismantling of zero-covid restrictions before authorities were ready. Groundless accusations of colluding with foreigners or causing the coronavirus outbreak stigmatize protesters, said Chih-Jou Jay Chen, professor of sociology at Academia Sinica in Taipei, Taiwan. “The party has total control of the legal system to prevent protesters from getting a fair trial,” especially if they are labeled “hostile forces,” Chen said. One widely shared post on the microblog site Weibo said the government was not at fault for a lack of preparation and urged people to focus their anger on those “who attacked and then scurried away,” asking, “Why shouldn’t they be reported to the authorities?”
Return to Top	

HEADLINE	**01/04 SEA ranks #8 top-performing global airports**
SOURCE	**https://komonews.com/news/local/seattle-tacoma-international-airport-seatac-travel-holiday-punctual-on-time-departure-top-performing-cirium-2022-airline-cancel-delay-delta-united-american-alaska-punctual#**
GIST	SEATAC, Wash. — Despite a holiday season filled with delayed and canceled flights, Seattle-Tacoma International Airport (SEA) was one of the most punctual in the world in 2022. SEA ranked No. 8 in Cirium's list of top-performing global airports of 2022. The online tracker's on-time rankings were calculated by on-time departures — a flight that arrives within 15 minutes of the scheduled gate arrival — and total flights. According to Cirium, 81.04% of SEA's flights boasted on-time departures out of 383,250 total flights, good for fifth place among American airports.

	Tokyo's Haneda Airport (90.33% on-time departures), India's Kempegowda International Airport (84.08%), Salt Lake City International Airport (83.87%), Detroit Metropolitan Wayne County Airport (82.62%), Philadelphia International Airport (82.54%), Minneapolis-St. Paul International Airport (81.95%) and India's Indira Gandhi International Airport (81.84%) finished above SEA. Colombia's El Dorado International Airport (80.72%) and Charlotte Douglas International Airport (80.68%) rounded out the top 10. Brazil-based Azul Airlines, with an on-time arrival rate of 88.93%, was named the top-performing airline globally. Delta (83.63%) and United (80.46%) ranked No. 5 and No. 8, respectively, worldwide. Following Delta and United among North American airlines were Alaska (80.36%), American (78.29%), Southwest (74.06%). Frontier (68.32%), JetBlue (66.35%), Allegiant (65.93%), WestJet (59.10%) and Air Canada (54.51%). "During 2022 airlines had difficulty anticipating the sudden recovery in demand," Cirium CEO Jeremy Bowen said in a statement. "They had been disappointed on several previous occasions throughout the pandemic, when it looked like demand was picking up, only for it to reverse course in the face of new Covid variants. When the recovery finally came this past year, the industry—including airlines, airports, air navigation providers and other stakeholders—struggled with understaffing and insufficient capacity. Delays and cancellations became issues. "In time, however, operations greatly improved as the industry added workers and adjusted capacity. 2023 appears to hold great promise for the aviation industry."
Return to Top	*Click here for the full report from Cirium.*

HEADLINE	**01/04 For Russia troops: cellphone use lethal**
SOURCE	**https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html**
GIST	Early in their invasion of Ukraine, some Russian fighters closing in on the capital, Kyiv, made calls with cellphones and uploaded videos to TikTok, betraying their location to Ukrainian eavesdroppers. The Ukrainians used the cellphone signals to launch missiles at their location — to devastating effect, according to Ukraine's head of military intelligence. Now, almost a year later and despite a ban on personal cellphones, Russian soldiers in the war zone are still using them to call wives, girlfriends, parents and each other, and still exposing themselves to Ukrainian attacks. After a strike that killed dozens — possibly hundreds — of Russian soldiers this week, one of the deadliest since the invasion began, the Russian military itself acknowledged the problem, using it to explain the heavy losses. "It is already clear that the main reason of what took place included the massive use, contrary to the ban, of personal mobile phones in the range of enemy weapons," the Russian Defense Ministry said in a statement. The cellphone data allowed Ukraine, it said, to "determine the coordinates of the location of military service members to inflict a rocket strike." Both a Ukrainian official and a group of Russian pro-war bloggers say other factors contributed to the strike, and that the ministry was trying to deflect blame from military leaders by casting it on soldiers. Russian commanders had housed a large number of troops together rather than dispersing them, stationed them near munitions that detonated in the attack, and failed to sufficiently disguise their movements, they said. But the use of personal cellphones has plagued both Ukraine and especially Russia throughout the war, leaving troops vulnerable to a piece of technology that, however mundane and ubiquitous in daily life,

can pose an existential threat in modern war.

Ukrainian officials say that Russian-backed forces have used cellphone data to target Ukrainian soldiers since at least 2014, when pro-Kremlin separatists began to fight Ukrainian troops in Ukraine's east.

The separatists debuted some of Moscow's newest forms of electronic warfare, Ukrainian officials say, and Ukrainian soldiers came to believe they were being targeted because soldiers — often in groups — were using their cellphones in proximity to one another. An artillery barrage on their position would soon follow the calls.

Almost a decade later, both Ukraine and Russia have honed their skills at using cellphone and radio signals as an effective targeting tool. While some Russian and Ukrainian units follow strict rules and ensure that cellphones are nowhere near frontline positions, social media posts from the battlefield show that cellphones are common among soldiers on both sides, and that efforts to keep them away are uneven at best.

The extent of Ukraine's resulting losses are unclear, but they appear to be less severe than Russia's. New York Times interviews with Russian soldiers and recorded phone calls intercepted by Ukrainian law enforcement throughout the war and obtained by The Times show that Russian commanders have tried, repeatedly, to keep phones off the battlefield.

Just before the invasion, Russian soldiers stationed in Belarus were told to give up their phones, two soldiers said in interviews. In intercepted calls, Russian soldiers can be heard saying that commanders confiscated their phones in February.

But just as often, soldiers found ways to circumvent the rules. They stole phones from Ukrainians, including those they had killed, and passed around the available phones to call home, an analysis of call logs shows. In many intercepted calls, Russian soldiers can be heard complaining that they did not trust their leaders or felt abandoned by them, and saying that they did not care about the rules.

Some Russian soldiers made remarks that showed they were aware Ukrainian intelligence could be listening — and that they should choose their words carefully, to avoid giving away their locations. But the soldiers did not appear to know that cellphone data alone could potentially betray them, giving Ukrainians enough to pinpoint a phone's location down to an apartment building.

"Fighting against phones at the front in the 21st century is just as useless as fighting against prostitution, for example," a widely followed, pro-war Russian blog on the Telegram app said on Wednesday. "It was, it is, and it will be."

The anonymous blogger said the use was not necessarily frivolous — for example, Russian troops had used their phones to post messages on Telegram to direct artillery fire.

Some Russian generals spoke over unsecure phones and radios early in the war, according to current and former American military officials, enabling the Ukrainians to locate and kill at least one general and his staff through an intercepted call.

But the generals changed tactics after those strikes, analysts say, and high-ranking commanders appear to use safer communications than ordinary troops, an analysis of call logs shows. The commanders' phone numbers and those of their family members, for example, are conspicuously absent from call logs that The Times obtained from the Kyiv region in March, and Ukrainian officials say the commanders use an encrypted network.

Ukrainian soldiers believe the Russians look for Ukrainian cellphones "handshaking" with individual cellphone towers. Once either side establishes a pattern or locates the concentration of forces on their phones by other means such as drones, artillery strikes frequently follow.

	In April in the eastern village of Husarivka, then just three miles from the front, a group of civilians found a spot in their tiny enclave where they could get cellphone service. But not long after a dozen or so residents congregated there to make calls, artillery shells started to rain down. The pattern repeated itself to the point that almost everyone in the town kept their phones off or in airplane mode, and avoided gathering in any place for too long. Despite the persistent threat, soldiers on both sides continue to hang on to their phones. The Ukrainians often have access to Starlink satellite internet near the front line, meaning calls do not use cell towers and are usually safe. But even without Starlink, the pull to be connected to home and to family — especially in such a brutal conflict, where even the home front is targeted by Russian missile strikes — is sometimes too powerful for Ukrainian troops to resist. The United States and its allies have watched the breakdown of discipline with some concern. In Iraq and Afghanistan, the locations of American troops and their allies were largely known to their enemies, who did not have the long-range weapons that have dominated the war in Ukraine. There were only hints about the havoc that personal technology might accidentally create, as in 2018, when data from a fitness app revealed the locations and habits of U.S. military bases and personnel, including those of American forces in Iraq and Syria. "What we didn't worry so much about 30 years ago now is every time you press a button you're emitting," Gen. David H. Berger, commandant of the Marine Corps, said last month in remarks to the Defense Writers Group. He said that commanders were acutely aware that young service members had grown up with cellphones, and that their habits were deeply ingrained. "They don't think anything about pressing a button," he said. "This is what they do all day long. Now we have to completely undo 18 years of communicating all day long and tell them that's bad. That will get you killed."
Return to Top	

HEADLINE	**01/05 Ukraine: Russia troops' sexual war crimes**
SOURCE	**https://www.nytimes.com/2023/01/05/world/europe/ukraine-sexual-violence-russia.html**
GIST	KHERSON, Ukraine — On her eighth or ninth day in Russian detention, Olha, a 26-year-old Ukrainian, was tied to a table, naked to the waist. For 15 minutes, her interrogator leveled obscenities at her, then threw a jacket over her and let seven other men into the room. "It was to frighten," she remembered. "I did not know what would come next." Sitting in Olha's cramped kitchen weeks later in Kherson, in southern Ukraine, Anna Sosonska, an investigator with the prosecutor general's office, listened to her recount the ordeal — an account of forced nudity that, prosecutors say, added to an accumulation of evidence that Russian forces had used sexual crimes as a weapon of war in the places they once ruled. "We are finding this problem of sexual violence in every place that Russia occupied," said Ms. Sosonska, 33. "Every place: Kyiv region, Chernihiv region, Kharkiv region, Donetsk region and also here in Kherson region." After months of bureaucratic and political delays, Ukrainian officials are gathering pace in documenting sexual crimes, which are prevalent and devastating in times of war but often remain hidden under layers of shame, stigma and fear.

“We found all types of cases of war crimes: rape, forced nudity, sexual torture” inflicted on men, women and children, Ms. Sosonska said. A pattern to the crimes is emerging, she added. “Now we see there is a line of war crimes in the Russian Army and among Russian commanders.”

Russian officials have repeatedly denied accusations of human rights abuses, despite widespread evidence and accounts collected by Ukrainian and international investigators. A spokeswoman for Russia’s Foreign Ministry, Maria Zakharova, recently dismissed a report by the U.N. Human Rights Commission as unsubstantiated testimonies and no more than “rumors and gossip.”

After investigating some areas Russia retreated from, an independent international commission reported to the United Nations in October that “an array of war crimes committed in Ukraine” included cases of sexual violence against women and girls.

Victims ranged from older than 80 to as young as a 4-year-old girl forced to perform oral sex on a soldier, which is rape, the report said. It detailed more than a dozen cases involving gang rapes, family members forced to watch a relative being sexually assaulted and sexual violence against detainees.

Iryna Didenko, who leads the prosecutor’s department investigating such crimes, has already opened 154 cases of conflict-related sexual violence. The real number, she said, is “much, much more.”

In one formerly occupied village in the Kyiv region, psychologists found one in nine women had experienced sexual violence, she said. Hundreds of people suffered sexual violence and torture in Russian detention, she added.

The trauma is raw and inhibiting. Viktoriya, a 42-year-old woman in the Kyiv region, shakes when she describes how, in early March, Russian soldiers shot dead her neighbor and then hauled her and her neighbor’s wife off to be raped.

“The fear still remains,” she said. “Sometimes when the electricity is out, I am seized by fear and I feel they could come back.”

Viktoriya was one of the few survivors willing to talk publicly. She asked that only her first name be used and that her face not be photographed, as did several other women, for fear of reprisals by Russian forces.

But the stigma and judgment of neighbors and acquaintances were also an abiding pain, she said.

“They are gossiping about me, and I mostly stay at home,” she said.

The grief was such that her neighbor Nataliia, who was also raped and whose husband was killed, was given refuge abroad. Her 15-year-old son was suicidal in the weeks after the attack, said Ms. Didenko.

A psychologist and lawyer, Ms. Didenko met Nataliia when she visited their village after Russian troops withdrew. Before the war, her department had handled domestic violence crimes, and she knew well the difficulties women faced in reporting crimes, she said.

Much of that has to do with the stigma of rape in a conservative religious society, but there is also a deep-seated distrust of the authorities in a post-Soviet system that has rarely focused on victims’ needs and often blamed them instead.

“From our experience with domestic violence, we realized victims do not talk about it in principle,” Ms. Didenko said. It is even harder in a war when they could be accused of fraternizing with the enemy, she said.

“No one will come running to apply to us,” she said. “That’s why we decided that we have to go to them.”

The need to help Ukraine's survivors of sexual violence is immense, activists say. The nation's few women's shelters have started taking in war victims. Aid organizations such as Women for Women International and the Andreev Foundation started providing mobile gynecological clinics and counseling sessions.

Of more than 800 woman and girls that the foundation has counseled since the invasion began, 22 have acknowledged experiencing sexual violence in the war. Eight were younger than 18.

Some survivors have expressed suicidal thoughts, said Anna Orel, an assistant project manager at the foundation. "One girl said that she wanted to cut off her own skin," she said. "She could not bear the smell of men's perfume."

Others were scared of military uniforms, even of Ukrainian soldiers, and of men in general.

"Many of them don't want to continue to live," Ms. Orel said. "It's very, very important for some professional person to hold their hand and to go through this with them."

From the accounts of those who have come forward, there is evidence that Russian commanders knew about rape or even encouraged it, officials said. Wayne Jordash, a British lawyer advising Ukrainian prosecutors, said he had seen signs of acquiescence by commanders among 30 cases he had reviewed.

Ms. Didenko said there was a clear pattern of behavior when Russian troops seized an area: "Ground forces arrive, and rapes start on the second or third day."

Witnesses reported commanders' ordering rape or giving instructions that suggested they condoned it, like telling soldiers to find some relaxation.

In one case Ms. Didenko described, a commander told his men, "OK, go," as he waited outside a house. One soldier was heard saying, "We'll just beat her," about one woman, and "This one we'll rape."

In another case, eight Russian soldiers raped and assaulted a man who was stopped at a checkpoint.

"These are not single cases," Ms. Didenko said.

There is an even clearer pattern, she said, of organized sexual abuse in the detention facilities run by Russian troops, police officers and security forces.

Investigators have found at least four large detention facilities in Kherson City, with graphic evidence of systemic torture under Russian occupiers.

In a business center's basement, detainees slept on pieces of cardboard in complete darkness and carved tallies to count the days and messages into the wall. "Oh God, give strength," one read.

"This was the torture room," said Yaroslav Manko, 30, a prosecutor from the region. The police found a rubber baton, metal handcuffs and an electric grill that Mr. Manko said was used to burn detainees' fingers. They also found a list naming Russian officers who had worked there.

There was extensive sexual abuse in the detention centers, including rape with batons and electric shocks to genitals, prosecutors and city officials said.

Olha, the Kherson woman, said that over 14 days in detention this fall she was threatened with rape, and that she was punched and kicked in the head and chest, breaking a rib. Russians put clamps on her legs, arms and earlobes to send an electric current through her body, she said, and doused her in water to worsen the shocks.

Her interrogators knew she worked with volunteers bringing aid from Ukrainian-held territory to civilians

	in Kherson. They demanded she film a propaganda video and distribute supplies in the name of United Russia, President Vladimir V. Putin's governing political party. Another activist, Andriy, 35, was held for five days in August. Russian occupiers accused him of helping underground partisans and demanded he give up his friends and acquaintances. "They give you electric shocks, then you're given a rest," he said. "Recovering, they beat you with batons or fists." The bruises on his back were shaped in a Z, a symbol of Russian fighters in Ukraine, he said. The electrical shocks to his earlobes knocked him unconscious. The shocks to his genitals still cause pain four months later. The similarity of the evidence and accounts across cities, describing torture methods, interrogations and officers from Russia's main intelligence agency, the F.S.B., has convinced Ukrainian prosecutors that abuses can be traced to the Russian leadership. "It cannot be that a soldier did this without an order," Ms. Didenko said. The F.S.B. "came efficiently, knowing their job, tortured everyone on the genitals" she said. "It's surely a system." Many Ukrainians and their supporters say they believe Russia aims to crush Ukraine's spirit of resistance and destroy its society. "It's part of a genocide," Ms. Didenko said, "but for us to prove it, we need time."
Return to Top	

HEADLINE	**01/04 Ukraine: Russia suffers heavy losses**
SOURCE	**https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-strikes.html**
GIST	KYIV, Ukraine — Ukraine has claimed a string of successful artillery attacks on Russian barracks in the first days of the year, asserting that it hit newly drafted men and other soldiers where they were sleeping or congregating, killing or wounding more than 1,000. The Russian military has confirmed one of the three waves of claimed strikes, though it gave a much lower death toll than the Ukrainians estimate. Even the lower toll of 89 soldiers killed in that attack, however, represents a startling setback for the Russian military. Social media posts, reports from local residents and Russians who blog about military affairs offered partial confirmation of the other strikes claimed by Ukraine, but not corroboration of the casualty counts. Military analysts say the Ukrainians' use of long-range artillery, including American-provided HIMARS precision rockets, to target barracks marks a shift for the artillery forces, which for months had concentrated on matériel like ammunition depots. The Ukrainian military's focus on the Russian infantry is among the first changes seen in its tactics with its American-provided weaponry, in response to Russia's mobilization of hundreds of thousands of soldiers over the fall. The haphazard movement of additional soldiers into the war zone, many of them poorly trained and led, has presented new targets behind the front lines for howitzers that can fire more than 20 miles and HIMARS rockets with a range of up to about 50 miles, analysts say. The Russian authorities say that draftees' use of personal cellphones on New Year's Eve helped the Ukrainians pinpoint a vocational school, being used to house soldiers, that was hit in the city of Makiivka in eastern Ukraine. Ukraine said the attack killed or wounded several hundred soldiers, while the Russians reported 89 dead. The casualty estimates could not be independently confirmed, and militaries often exaggerate the losses of their enemies and downplay their own. But in this instance, images of the pancaked vocational school, and the Russian military's confirmation of serious losses, showed a well-planned strike.

In the ensuing days, the Ukrainian military claimed two more attacks directed at an array of towns in the Kherson and Zaporizhzhia regions of southern Ukraine, claiming a total of about 1,200 casualties in all three sets of strikes together. It was far from clear how reliable the claims were.

The Russians played down the damage in Zaporizhzhia and Kherson, but residents in nearby areas of the occupied territory told Ukrainian officials that they had heard loud explosions around the time of the claimed strikes.

A New York Times analysis of video footage confirmed severe damage at a veterans association in Tokmak that was annexed to a hospital complex, as well as the partial destruction of a four-story building alongside a commercial street in Vasylivka. Both cities, in the Zaporizhzhia region, were locations the Ukrainian military said it had struck. It was unclear whether any of these buildings were housing Russian soldiers.

The Ukrainian casualty claims may be intended in part to unnerve the enemy.

On Friday, Ukrainian officials issued a warning that appeared to be part of a campaign to encourage men in Russia to evade the draft: Much of Russian-occupied southern Ukraine, they said, now lies within range of Ukrainian artillery.

“Given that our foreign partners supply us with new types of weapons, the so-called land corridor to Crimea is certainly not safe,” Andriy Cherniak, a spokesman for Ukraine’s military intelligence agency, told the Ukrinform news agency Wednesday. The reference was to the area along the Sea of Azov linking southern Russia to the occupied Crimean Peninsula, a swath of land Russia seized early in its invasion.

Serhiy Hrabsky, a former colonel in the Ukrainian military who is now commentator for Ukrainian media, said the recent strikes suggested that Ukraine had begun trying to target conscripted soldiers as they deploy.

“We see a large concentration of Russian troops on the front lines now,” Mr. Hrabsky said.

Lacking sufficient trucks and other vehicles to disperse soldiers within range of Ukrainian missiles, he said, Russian commanders have left large groups congregated — and vulnerable. “They need to concentrate them just to move them from point A to point B,” Mr. Hrabsky said.

Russian bloggers who cover the war, and offer a more unvarnished lens on the Russian military than state media, generally played down the strikes in southern Ukraine despite sharply criticizing the Russian military command for the acknowledged attack in Makiivka.

But the bloggers did circulate a video on New Year’s Day showing a heavily damaged building that The Times geolocated to a country club about 28 miles from a town where the Ukrainian military said it had struck troop congregations.

Several military bloggers said that a Russian volunteer may have inadvertently exposed the location of the site, the Grand Prix Country Club, by posting on social media. A man using the name Petr Lozhkovoy posted online pictures of the site in November and December and said Russian special forces were present.

The Russian defense ministry has not commented on any other strikes apart from Makiivka. Pro-war Russian correspondents and occupation authorities offered limited details of the other attacks, saying military losses were minimal while highlighting civilian collateral damage.

Two prominent Russian military social media channels confirmed a Ukrainian strike in the Chulakovka area of Kherson region on New Year’s Eve, without providing casualty estimates. The Telegram channel Grey Zone, which is affiliated with Russian mercenary group Wagner, said the strike hit a farming complex near the village but provided no other details.

	A review by The Times of medium-resolution satellite imagery of Chulakovka, as well as the farming complex, did not show any detectable damage caused by a strike, though that does not mean one did not occur. Radio Liberty cited a local official from the town as saying that explosions had been heard in the area of a pig farm where Russian soldiers had been garrisoned. During a strike in the Zaporizhzia region on Jan. 2, residents of nearby towns reported hearing a loud explosion, Dmytro Orlov, the exiled mayor of the Russian-occupied city of Enerhodar said in a telephone interview. Pro-Russian bloggers posted about strikes in the region two days after the Ukrainian military announced the attacks, and claimed that civilian sites, including a hospital, had been hit.
Return to Top	

HEADLINE	**01/04 China's unfolding tragedy**
SOURCE	**https://www.nytimes.com/2023/01/04/briefing/chinas-unfolding-tragedy.html**
GIST	In early December, China suddenly reversed its "zero Covid" policy. That set off a wave of infections that has swept across the nation, overwhelming hospitals and funeral parlors. Two events this month could further inflame the already raging outbreak. On Sunday, the country will reopen to tourists, and visitors will no longer be required to quarantine upon arrival. A few weeks later, China will celebrate Lunar New Year, the country's biggest holiday — typically the largest annual migration of people on the planet. For insight into the situation in China, I spoke with Keith Bradsher, The Times's Beijing bureau chief. This interview has been edited for length and clarity. **For those who aren't familiar, what was life like in China before the restrictions were removed?** Almost overnight, the rules changed on Dec. 7. Until then, people were at constant risk of being sealed in a hospital room for weeks if they caught a Covid infection. Until Dec. 7, people who even went to the same shop or eatery as someone who later turned out to be infected, or even passed an infected person on the street, could end up being taken away to a quarantine center for a prolonged stay, sometimes with meager food and sanitation, or sealed in their homes. In big cities like Beijing or Shanghai or Shenzhen, it became necessary to line up every two or three days and sometimes daily at sidewalk booths for P.C.R. tests, all tracked by the health codes on our cellphones. Because of the extreme sensitivity of the tests, an infected person could be kept in isolation for weeks or even months. And even after people left quarantine they could face permanent discrimination. There were some places that you weren't allowed to go if you ever had Covid, like some government offices. **So what do things look like now?** After Dec. 7, life was transformed. The good news was that we could suddenly move around without worrying about being locked up in a hospital or quarantine center. But the cost in illness and death has been high. We went from medics being responsible for detaining people to suddenly caring for a lot of sick people. We've gone from funeral homes allowing lengthy services for as many as 100 guests to lacking adequate cremation capacity and barely allowing immediate family members to say goodbye. We've seen hospitals practically overflowing, with little space left for more sick people. There's an acute shortage of ventilators. There is an acute shortage of ibuprofen. Even hospitals don't have enough

ibuprofen to bring down the fevers of the very sick.

All of these are scenes that were witnessed in the West when the pandemic first emerged in early 2020. But in China, it has been a surprise that there were not more preparations for the change in direction.

What do you mean?
The vaccination program nearly ground to a halt in late spring without ever reaching many of the country's older adults, who tended to resist vaccination. Many thought they could hide indefinitely from the virus. Their faith in China's vaccine industry had also been damaged by vaccine scandals before the pandemic, even though there is no evidence of safety problems for the Covid vaccines.

The spread of the virus is extraordinary because not only do you have a population with almost zero past exposure or immunity, but now — in a policy about-face — you have towns encouraging people to come to work even if they are positive for Covid, as long as they are not especially feverish. I've been talking to companies in northern China, and some have told me that anywhere from 80 to 100 percent of their staff members have been infected.

Why did China change its policy so quickly?
China faced several big challenges. There was mounting domestic unhappiness with the burden of quarantine and frequent testing, which resulted in street protests. China was also losing control of the virus even before the policy change on Dec. 7. The death rate began to spike upwards right after the loosening of restrictions, even though it takes the virus a couple weeks to reach the fatal phase. The immediate jump in activity at funeral homes suggested that there were a lot more people who were infected right before the policy change but were hiding at home.

Finally, the economy was in terrible shape through the autumn because people in China stopped going out to shop or to restaurants for fear of being infected. At the same time, overseas demand for goods from China was withering.

How are the Chinese people feeling?
Absolutely everyone seems to know some elderly person about whom he or she is deeply worried right now — because the threat of serious illness from Covid increases with age. The country is experiencing a terrifying surge, and yet cities are encouraging travel for Lunar New Year, which starts in less than three weeks. We will likely see surges in rural areas, where many of the residents are elderly.

What would a rural surge look like?
There was a study back in 2007 by the agriculture ministry which surveyed 3,000 villages. They found that in 90 percent of those villages, there were essentially no able-bodied people between the ages of 16 and 40 who had stayed. Almost all had gone to the cities to find jobs. So rural areas often have lots of grandparents raising grandchildren while the middle generation works in the cities. The fear is that just as the virus has raced through the population in Chinese cities, it will now race through Chinese villages in the next several weeks.

The other scary part in all of this is that this is the first wave, and it's mostly being driven by earlier versions of Omicron. So people in China are acquiring resistance to Omicron subvariants that are already fading away globally. As China reopens its borders in the coming weeks, there is a possibility that the latest immune-evading subvariants may come next, as they have already become prevalent in parts of the United States. If that happens, residents may face further illness instead of a hoped-for single wave that quickly disappears.

What will China's reopening mean for the course of the pandemic?
It's unclear that this will cause new variants to emerge. Some scientists have said that what's happening in China is less likely to affect the rest of the world because it's basically exposing a low-immunity population to variants that have already circulated a lot globally.

I think the tragedy here is less of a global tragedy and more of a tragedy of China. It's a tragedy of the

	loss of so much of its older generation, which is now being sacrificed in a race to reopen and restart the economy quickly.
Return to Top	***Understand the Situation in China*** *The Chinese government cast aside its restrictive "zero Covid" policy, which had set off mass protests that were a rare challenge to Communist Party leadership.* • ***Rapid Spread:*** *Since China abandoned its strict Covid rules, the intensity and magnitude of the country's outbreak has remained largely a mystery. But a picture is emerging of the virus spreading like wildfire.* • ***Economic Recovery:*** *Years of Covid lockdowns took a brutal toll on Chinese businesses. Now, the rapid spread of the virus after a chaotic reopening has deprived them of workers and customers.* • ***A Failure to Govern:*** *China's leadership likes to brag about its governance of the country, but its absence in a moment of crisis has made the public question its credibility.*

HEADLINE	**01/04 More toy recalls than last 4yrs combined**
SOURCE	**https://www.washingtontimes.com/news/2023/jan/4/more-toys-recalled-2022-previous-4-years-combined/**
GIST	An inflatable inner tube with poles covered in lead-based paint. A toddler walker with tiny wheels and wheel attachment hardware that can detach. A "stacking" activity set with information stickers that can separate from the bottom. These were some of the most searched-for recalled toys in 2022, as more toy recalls were issued last year than in the previous four years combined. The U.S. Consumer Product Safety Commission issued 30 toy recalls in 2022 — up from nine in 2021, two in 2020, three in 2019 and six in 2018. The commission also worked with border agents to seize millions of illegal imported toys. Choking hazards prompted the last two recalls on Dec. 1, when Target flagged 23,400 units of the Cloud Island 4-Piece Plush Toy Sets and HABA USA recalled about 800 Discovery Cubes Animal Hide and Seek activity toys. Target said consumers should immeidately take the stuffed toys away from their children and return them for a refund. Asphyxiation among infants and toddlers causes most deaths involving recalled toys. According to the safety commission's most recent data, emergency rooms treated more than 152,000 toy-related injuries to children younger than 15 in 2021. They included two deaths: a 17-month-old boy who choked on an egg-shaped plastic toy and an 8-month-old girl who suffocated while sleeping face-down on a soft toy. In an email to The Washington Times, commission press secretary Patty Davis pointed to a surge of toys brought into the U.S. without proper safety testing. Ms. Davis referred to a November report saying the commission helped Customs and Border Protection confiscate about 2 million "dangerous or illegal toys and children's products" entering U.S. ports last year. That included nearly 300,000 seizures for lead-related issues. "We are committed to doing our part to ensure, through vigorous inspections and enforcement, that hazardous products don't make it to store shelves or consumers' homes," commission Chair Alexander Hoehn-Saric said in November. The most-sought recalled toy in 2022 was the Jungle Jumparoo. Children could jump up and down on an inflatable inner tube while grasping vertical poles in the center. The toy maker recalled about 350 of them in June after learning that a small batch had yellow poles with potentially toxic amounts of lead. More than 18,300 people searched online for the Jungle Jumparoo recall last year, Australian gift company Yellow Octopus found in an analysis of Google Trends data. More people searched for details about the Jungle Jumparoo recall than the rest of the top five toy recall searches combined, according to Yellow Octopus.

	"The toys' yellow poles contain levels of lead that exceed the federal lead content ban. Lead is toxic if ingested by young children and can cause adverse health issues," the Consumer Product Safety Commission says in the recall notice posted online. All affected consumers received a letter to request two replacement poles, a Jungle Jumparoo customer service representative said, adding that the company typically receives one to three returns a year. "We have also implemented procedures in our manufacturing process to avoid any potential issues in the future," the spokesperson said in an email. "We have had virtually no returns of our product post-Christmas." The second most searched recall, at 5,770, was for Walk 'n' Learn Wooden Activity Toddler Walkers. The company recalled about 17,200 of the walkers in March after problems with the wheel and wheel attachments created a choking hazard. In November, Professor Puzzle recalled 2,350 units of its Children's Rainbow Stacking Toy because of reports that the sticker detached and created a choking hazard. That sparked 2,030 Google searches for information, Yellow Octopus reported. The Consumer Product Safety Commission urges consumers who suspect they bought a recalled toy to search the agency's website for replacement, refund and repair options. Federal safety standards mandate the testing of toys sold in the U.S. for eight potentially toxic elements, including lead. Toy companies enforce the standards and initiate most government recalls before any injuries occur, said Alan P. Kaufman, senior vice president of technical affairs for the Toy Association. Problems sometimes arise from batches of toys manufactured overseas without appropriate testing, said Mr. Kaufman, who specializes in toy safety standards for the industry. "We have not noticed an increase in safety issues with toys from legitimate sellers," Mr. Kaufman said in an email. "But consumers need to be cautious about purchasing counterfeit toys or toys from illegitimate sellers, which are often not designed, manufactured, and tested to the high standards that the industry adheres to."
Return to Top	

HEADLINE	**01/04 SKorea stands up offensive drone unit**
SOURCE	**https://www.washingtontimes.com/news/2023/jan/4/south-korea-stands-offensive-drone-unit-after-nort/**
GIST	SEOUL — South Korean President Yoon Suk Yeol ordered his military to establish a joint command drone unit 10 days after North Korean drones dramatically exposed vulnerabilities of his nation's skies. The South's commitment Wednesday to a response of sending two or three drones north for each drone the North sends south raises questions about Seoul's compliance with the armistice that halted the 1950-1953 Korean War. After a briefing from the Agency for Defense Development, the joint chiefs of staff, the National Defense Ministry and the presidential National Security Office, Mr. Yoon ordered Defense Minister Lee Jong-sup to establish a joint drone command to oversee surveillance and reconnaissance operations. Mr. Yoon also ordered the mass production of small drones and the accelerated development of stealth drones, the Yonhap News Agency reported. Although South Korean military units already operate drones, the new command will operate "at the

strategic and operational level that is different from the existing drone battle level," the Defense Ministry said in a media release. It will "carry out operations in all areas beyond the army's command level."

The conservative Mr. Yoon also suggested that if the North continued drone intrusions, the South should consider revoking a 2018 military agreement with the North to reduce tensions. That deal was signed by his presidential predecessor, the liberal Moon Jae-in.

The presidential office in Seoul said North Korea explicitly violated the agreement 17 times, including 15 times since October, Yonhap reported.

Left unmentioned was the drone command's potential impact on the 1953 armistice. That deal has maintained an uneasy peace on the peninsula for seven decades. Drone flights over the Demilitarized Zone separating the two Koreas, even in retaliation for incursions, would violate the armistice, analysts said.

Pyongyang's provocations shocked South Korea, which is customarily blase about its northern neighbor's hostilities.

On Dec. 26, five North Korean drones penetrated South Korean airspace. Four flew over Paju, the county north of Seoul and south of the DMZ, and one over Ganghwa Island in the Yellow Sea. One flew as far as Seoul's northern metropolitan area.

Paju is dense with military facilities, including the U.S. military's 2nd Infantry Division's base, and Ganghwa Island is strategically located.

South Korean aircraft and helicopters scrambled and fired more than 100 live rounds. A light attack aircraft crashed while taking off, although no casualties were reported.

South Korean drones were dispatched – for the first time, as far as is known – north of the DMZ on a retaliatory surveillance operation.

All the North's drones disappeared from South Korean radars, but no wreckage was discovered. All five apparently returned successfully to the North. The South Korean military said it was limited because the drones were small, made irregular maneuvers and were not launched from an airfield.

Perhaps most worrisome was the necessity to briefly halt flights at Seoul's two commercial airports, in Incheon and Gimpo, for more than an hour. That potentially handed Pyongyang a low-cost, low-risk weapon to wage economic war against the South.

The inability of South's high-tech military to take down the drones created widespread shock.

On Dec. 27, Mr. Yoon ordered the deployment of two or three drones into North Korea for each drone North Korea sends south, though no intrusions have been reported since Dec. 26. On Dec. 29, South Korea conducted drone defense drills involving unmanned aerial vehicles, attack helicopters, light attack aircraft, 20 mm cannon and short-range surface-to-air missiles, or SAMs.

The military response could create a diplomatic headache.

"The context of this discussion is that, with South Korea responding the way it is being implied right now, it is not adhering to the armistice agreement," Chun In-bum, a retired South Korean lieutenant general, told The Washington Times. "So we find ourselves at the same level as the North Koreans."

Steve Tharp, a retired U.S. Army lieutenant colonel, said in an interview that a principle of reciprocity exists. Even so, "anytime you fly into the airspace of the other side, that is a violation of the armistice," Mr. Tharp, who has negotiated extensively with North Koreans, told The Washington Times.

The U.S.-led U.N. Command, which oversees the DMZ, did not respond to a request for comment.

	Drones are hardly invulnerable. Ukrainian forces have fought off an onslaught of Russian- and Iranian-made attack drones with electronic jamming, SAMs, radar- and searchlight-guided ground fire, massed small arms and other measures. Yet Seoul and its environs, densely populated and just 37 miles from the DMZ, presents a particularly tough defensive challenge, and its commercial air volume dwarfs that of Pyongyang. Even debris shot down from an intercepted enemy drone is likely to fall onto sensitive or populated ground. "Unless we can control the downfall of a drone, it will crash into somebody or something," said Mr. Chun. "Collateral damage is our problem." Small, low-cost drones are ideal asymmetric tools for the impoverished North to deploy against the prosperous South. "A drone can take out a tank – what an investment that is," Mr. Tharp said. "What does a drone cost – a couple of thousand dollars? A tank costs a few million."
Return to Top	

HEADLINE	**01/04 Govt. settles 'dreamer' detention lawsuit**
SOURCE	**https://www.thenewstribune.com/news/local/article270780027.html**
GIST	The federal government has reached a settlement with a 29-year-old man who argued he was wrongfully held at the immigration detention facility in Tacoma, the U.S. Attorney's Office announced Wednesday. Immigration officials arrested Daniel Ramirez Medina at his home in Des Moines in 2017. He was protected from deportation by the Deferred Action for Childhood Arrivals program at the time. He was held for six weeks at the privately owned and operated federal immigration detention center on the Tacoma Tideflats until an immigration judge ordered his release. "This settlement essentially gives Mr. Ramirez Medina a clean slate as he works to obtain legal status in the United States," U.S. Attorney Nick Brown said in a news release Wednesday. "I am pleased that this settlement involves no monetary payment and yet goes to the core of what Mr. Ramirez Medina wants: a fair chance to obtain legal status in the U.S." Ramirez Medina had no criminal history when he was detained, but immigration officials said he admitted to gang affiliations, which his attorneys said was false, The News Tribune previously reported. He was brought to the United States from Mexico when he was about 10, according to court records, and was protected from deportation under DACA starting in 2014. "The government targeted Mr. Ramirez despite its knowledge that he is a 'Dreamer' who was twice granted deferred action and work authorization under DACA after rigorous vetting," a complaint filed on his behalf in U.S. District Court in Seattle last year said in part. The complaint argued the government "falsely asserted that he was gang-affiliated, notwithstanding the total absence of any credible evidence to support that allegation, and continued to press for his removal long after it concluded that he posed no danger to the community." The settlement gives Ramirez Medina "a four-year stay of removal from the United States," the U.S. Attorney's Office news release said, and prohibits U.S. Immigration and Customs Enforcement officials from considering "any allegation that he is a gang member or a threat to public safety." The agreement settles Ramirez Medina's $450,000 tort claim, and "is not an admission of liability or fault by any of the parties," according to U.S. Attorney's Office.

	If Ramirez Medina breaks the law, the news release said, “the grant of deferred action can be terminated.” Attorneys who represented Ramirez Medina, according to court records, did not immediately respond to The News Tribune’s request for comment.
Return to Top	

HEADLINE	**01/04 High winds thru Seattle area; power loss**
SOURCE	**https://www.seattletimes.com/seattle-news/thousands-without-power-as-high-winds-hit-seattle-area/**
GIST	Thousands of Puget Sound Energy customers were without power Wednesday night as high winds marched into Western Washington. Winds were expected to increase across the Cascades on Wednesday night, with high winds into Thursday as a series of systems brewing off the coast move east. The strongest winds will be near the Cascade Gaps, according to the National Weather Service. About 13,500 customers were without power around 5 p.m., many of whom were in East Bellevue, Preston and North Bend. Around 2,700 customers scattered across Bellevue remained without power around 9 p.m. Nearly 1,500 customers in North Bend reported outages around 5 p.m., but the outage numbers fell to about 600 by 8:30 p.m. Thousands east of Puyallup along 410 lost power Wednesday evening as high winds blasted the Cascades. More than 1,500 customers lost power shortly after 8 p.m. in Enumclaw, with no estimated restoration time. Around 700 people were without power in Lake Tapps, where power was expected to be restored around 10 p.m. More than 600 people lost power around 7 p.m. in Buckley. A tree came down across all lanes of Northeast 116th Street in Redmond shortly before 8 p.m. because of high winds. No one was injured, but the westbound lane of 165th Place Northeast and the eastbound lane of 162nd Avenue Northeast were closed with no word on when they may reopen. Seattle City Light reported about 300 customers were without power just before 9 p.m. A large tree fell on 35th Avenue Southwest between Southwest Avalon Way and Southwest Snoqualmie Street in West Seattle, according to the Seattle Department of Transportation. It wasn’t immediately clear whether the tree was blown over by high winds.
Return to Top	

HEADLINE	**01/04 Windy, stormy conditions in western WA**
SOURCE	**https://www.seattletimes.com/seattle-news/weather/windy-wednesday-forecast-across-western-wa/**
GIST	A series of systems brewing off the coast will deliver stormy conditions to Western Washington through the end of the week. The first system made for a windy Wednesday, marching into the region with winds blowing east to west, according to the National Weather Service. The region saw winds from the Cascade foothills to the coast, NWS said. Puget Sound Energy reported power outages throughout the Seattle area Wednesday evening, mainly on the Eastside and along the Interstate 90 corridor. At 5 p.m., about 15,000 customers were in the dark, a number that fluctuated during the evening. A second system will push inland late Thursday into Friday, bringing more of the same windy conditions and an increased chance of rain.

	"Winds on Thursday are going to remain elevated across the area but gradually start to ease going into Friday," said Samantha Borth, a meteorologist with the weather service, "but you might see some breezy southerly winds, at least for a little bit early Friday morning." Seas will be stormy along the coast with swells near 17-19 feet and possible 20-foot waves as the system slides over the Pacific, according to the weather service. Highs for most of the Seattle area will climb a few degrees from Wednesday's mid-40s and top out in the upper 40s to low 50s. As winds blow through the region, rain will be widespread and light through Friday, with "more of a heavier rainfall west of the Sound," Borth said. If you're traveling through the Cascades, expect easterly winds and light snow to make roads slick this week. "Snow levels are going to be below pass level. What we're looking at is not too significant by any means, maybe 1 or 2 inches of snow through Thursday, and then some additional light accumulation Thursday to Friday," Borth said. During Wednesday's first weather system, the weather service issued a wind advisory for 30-40 mph winds and gusts up to 55 mph through 4 a.m. Thursday for areas along the Strait of Juan de Fuca and east Puget Sound lowlands. The same easterly wind blew through areas along the coast, with gale warnings in effect from 4 p.m. Wednesday through 4 a.m. Thursday for areas from Ocean Shores to Forks and the Strait of Juan de Fuca. Along the Interstate 5 corridor, conditions were calmer, with 15-25 mph winds and gusts up to 35 mph by Wednesday evening. NWS expected gusts to peak to 40 mph through Wednesday night in the Seattle area. Power outages and downed tree limbs are possible through Thursday, when winds are expected to subside. Another system will move into the region Friday into Saturday, bringing more rain and wind into Western Washington.
Return to Top	

HEADLINE	**01/04 Armed robbery spree: 15yr-old, 21yr-old**
SOURCE	**https://www.king5.com/article/news/crime/15-year-old-21-year-old-charged-armed-robberies/281-96e464f3-57c2-49e8-b390-03ba9fb170f5**
GIST	SEATTLE — Detectives are linking a 15-year-old boy and a 21-year-old man to an armed robbery spree in King County. The teen was arrested in November. The adult was taken into custody more than two weeks ago. The first charges filed focus on what police say happened on Nov. 17. That's when a call came in about two males, one armed with a gun, committing a robbery at a 76 gas station in Renton around 7:30 p.m. More than half an hour later, there was an attempted armed robbery at a Chevron gas station in Kent. Less than ten minutes after that, police say there was an armed robbery reported at a 76 gas station in Covington. Court documents say surveillance images helped investigators link a 15-year-old boy and a 21-year-old man to the three cases. "In the public court documents, we've heard that there may be many more cases, potentially dozens more cases, and Sheriff's Office Investigators are working on that right now," said Casey McNerthney, a

	spokesperson for the King County Prosecuting Attorney's Office. Determination of probable cause documents state that between Nov. 2 and Nov. 18, 37 individual armed robberies have occurred in south King County that allegedly appear to have been committed by the same people. "It's concerning when you see this kind of violence and the consistency of it. Regardless of your age, if you use a gun like this, you can expect King County prosecutors to act on it immediately," said McNerthney. The 15-year-old's case is going through the juvenile court system. Currently, he is charged with two counts of robbery, one count of attempted robbery, and unlawful possession of a firearm. The 21-year-old is charged with more than a dozen counts for an alleged crime spree that police say targeted businesses and gas stations. He is being held on $500,000 bail at the King County Correctional Facility.
Return to Top	

HEADLINE	**01/04 Health officials concern: new Covid variant**
SOURCE	**https://www.kiro7.com/news/local/local-health-officials-tracking-new-covid-omicron-variant-believed-be-more-contagious/DYZQEBTQTJHLZPQJBVFAZMNX7A/**
GIST	SEATTLE — A new year has brought concerns about a new COVID-19 variant. The XBB.1.5 variant is an offshoot of the omicron variant and is believed to be five times as contagious. The XBB.1.5 variant now makes up more than 40% of coronavirus cases in the US, according to the CDC. In parts of the northeast, like New York, it's believed to make up more than 70% of the cases. Dr. Pavitra Roychoudhury, a virologist with UW Medicine, believes Washington will also see a surge in the new variant. "Because of the amount of travel and mixing that's been happening over the last several months, I wouldn't be surprised if it catches up here as well. And this has happened in previous waves where we see a particular variant take off in one part of the country, and then soon after, it catches up elsewhere," said Dr. Roychoudhury. Though she adds that it will be difficult to know the exact case number because so many people now rely on at-home testing, and not everyone reports their positive test results to the state. She says that hospitalization rates will be the most accurate metric to determine the impact of XBB. 1.5. Hospitals across the nation have already seen a rise in COVID-related hospitalizations in recent weeks. The King County Health Department says hospitalizations have been relatively steady for the past month, but it's something their department will continue to monitor. In a statement to KIRO 7, the department writes, "We are concerned about the potential for XBB1.5 to lead to a surge, and although at this point, we can't be sure how severe that might be, we do not expect anything as severe as what we experienced last winter during the Omicron surge." However, the department does have some concerns about the new variant in regards to the vaccine, writing, "XBB1.5 is also concerning because it is not susceptible to monoclonal antibody treatments, although the antiviral drug Paxlovid remains effective and is important for those who are eligible and do develop COVID-19."

	Health experts have already started warning that vaccine boosters aren't as effective against XBB.1.5 as they were against the omicron variant. Dr. Roychoudhury said while the new variant poses some concerns, she doesn't want to instill a sense of panic, telling KIRO 7 that with masks, vaccines and information, the public is in a much better position than we were in 2020. "I totally get the exhaustion, and I totally get the confusion that comes from tracking all these variants that have increasingly complicated alphanumeric names. But we're in a really different place from the panic of 2020," said Dr. Roychoudhury. "I think we should be glad that we have the ability to track that this variant even is out there. That we're able to monitor it over time. And we're able to provide that sort of warning that, 'Hey, this is a this is a variant to watch out for.'"
Return to Top	

HEADLINE	**01/04 More job cuts in latest tech worker purge**
SOURCE	**https://www.kiro7.com/news/local/amazon-salesforce-jettison-jobs-latest-tech-worker-purge/F4E3DIUV2VDRHHOCYVIO5XCKFY/**
GIST	E-commerce giant Amazon and business software maker Salesforce are the latest U.S. technology companies to announce major job cuts as they prune payrolls that rapidly expanded during the pandemic lockdown. Amazon said Wednesday that it will be cutting about 18,000 positions. It's the largest set of layoffs in the Seattle-based company's history, although just a fraction of its 1.5 million global workforce. "Amazon has weathered uncertain and difficult economies in the past, and we will continue to do so," CEO Andy Jassy said **in a note to employees** that the company made public. "These changes will help us pursue our long-term opportunities with a stronger cost structure." He said the layoffs will mostly impact the company's brick-and-mortar stores, which include Amazon Fresh and Amazon Go, and its PXT organizations, which handle human resources and other functions. In November, Jassy **told staff that layoffs were coming** due to the economic landscape and the company's rapid hiring in the last several years. Wednesday's announcement included earlier job cuts that had not been numbered. The company had also offered voluntary buyouts and has been cutting costs in other areas of its sprawling business. Salesforce, meanwhile, said it is laying off about 8,000 employees, or 10% of its workforce. The cuts announced Wednesday are by far the largest in the 23-year history of a San Francisco company founded by former Oracle executive Marc Benioff. Benioff pioneered the method of leasing software services to internet-connected devices — a concept now known as "cloud computing." The layoffs are being made on the heels of a shake-up in Salesforce's top ranks. Benioff's hand-picked co-CEO Bret Taylor, who also was Twitter's chairman at the time of its tortuous $44 billion sale to billionaire Elon Musk, left Salesforce. Then, Slack co-founder Stewart Butterfield left. Salesforce **bought Slack** two years ago for nearly $28 billion. Salesforce workers who lose their jobs will receive nearly five months of pay, health insurance, career resources, and other benefits, according to the company. Amazon said it is also offering a separation payment, transitional health insurance benefits, and job placement support. Benioff, now the sole chief executive at Salesforce, told employees in a letter that he blamed himself for the layoffs after continuing to hire aggressively into the pandemic, with millions of Americans working from home and demand for the company's technology surging.

	"As our revenue accelerated through the pandemic, we hired too many people leading into this economic downturn we're now facing, and I take responsibility for that," Benioff wrote. Salesforce employed about 49,000 people in January 2020 just before the pandemic struck. Salesforce's workforce today is still 50% larger than it was before the pandemic. Meta Platforms CEO Mark Zuckerberg also acknowledged he misread the revenue gains that the owner of Facebook and Instagram was reaping during the pandemic when he announced in November that his company would by **laying off 11,000 employees,** or 13% of its workforce. Like other major tech companies, Salesforce's recent comedown from the heady days of the pandemic have taken a major toll on its stock. Before Wednesday's announcement, shares had plunged more 50% from their peak close to $310 in November 2021. The shares gained nearly 4% Wednesday to close at $139.59. "This is a smart poker move by Benioff to preserve margins in an uncertain backdrop as the company clearly overbuilt out its organization over the past few years along with the rest of the tech sector with a slowdown now on the horizon," Wedbush analyst Dan Ives wrote. Salesforce also said Wednesday that it will be closing some of its offices, but didn't include locations. The company's 61-story headquarters is a prominent feature of the San Francisco skyline and a symbol of tech's importance to the city since its completion in 2018.
Return to Top	

HEADLINE	**01/04 Mask mandates return to NJ schools**
SOURCE	**https://www.fox5ny.com/news/mask-mandates-return-at-several-nj-school-districts**
GIST	NEW JERSEY - Students in several school districts across New Jersey are back from winter break, and back to wearing masks in classrooms. Beginning Tuesday, students and staff in Paterson must wear masks indoors, along with students in the Passaic School District, which reinstated the policy before winter vacation. The Camden City School District also announced a mask mandate for two weeks at 18 of its schools. The move comes in response to the so-called "tripledemic," as cases of COVID-19, RSV, and influenza spike all around the region. The masks will remain on until further notice in Paterson. Passaic said it would lift that mask mandate when Passaic County is in the moderate or below range in the NJDOH COVID-19 Activity Level Report. Newark, the largest public school district in New Jersey, has not implemented a mask mandate.
Return to Top	

HEADLINE	**01/05 New XBB.1.5 variant 'spreading like wildfire'**
SOURCE	**https://www.foxnews.com/lifestyle/new-covid-omicron-subvariant-xbb-1-5-spreading-wildfire-us-health-experts-reveal-why**
GIST	The new omicron subvariant, known as XBB.1.5, is spreading like wildfire across the U.S. As colder weather brings in peak COVID infections, this novel mutation is beginning to worry health professionals. So, what are some of the unique features of the strain that is now gripping swaths of the country?

First, this subvariant is immuno-evasive. It's not as susceptible to natural immunity or vaccines — and it is very contagious, health professionals say.

In a phone interview with Fox News Digital, Fox News medical contributor Dr. Marc Siegel explained that there are actually two subvariants at play: XBB and XBB.1.5.

XBB.1.5 is more contagious, said Dr. Siegel, who is also a professor of medicine at NYU Langone Medical Center in New York City.

It's more contagious due to its ability to grip tightly onto a host, he explained.

"The spike proteins are like suction cups," he said.

"So, the more it can get a grip … the more easily it transmits from cell to cell," he added.

Both XBB subvariants are "highly contagious," Siegel added, since each omicron variant is "out-competing its predecessor."

Dr. Shad Fani Marvasti, associate professor and director of public health and prevention at the University of Arizona College of Medicine - Phoenix, told Fox News Digital that each new strain develops with the intention of overshadowing those that went before it.

"Viruses always want to be more and more transmissible and infect more hosts," he said.

In some cases, there's a "trade-off" between mutations, in which some may become more transmissible but less virulent in terms of the health impact, Marvasti also said.

This is the hope for omicron and its developing variants, such as the "sticky" XBB, he noted.

He said he hopes that "we start seeing [the variants becoming] less severe," he said.

"And that can be both a function of the evolution of the virus … and also the fact that more people have been exposed to the virus through either vaccination boosters or previous infections," he said.

Dr. Siegel added that so far there's "no evidence" that XBB is more virulent.

"If it's spreading like wildfire and it's not killing more people, that means it's less virulent," he said. "But we don't know the reason for that."

Currently, XBB.1.5 accounts for almost 41% of confirmed COVID-19 cases across the country, according to data from the Centers for Disease Control and Prevention (CDC).

The XBB mutation has picked up speed, jumping from just 21% of COVID-19 cases on Christmas Eve, the CDC noted.

During the last week of December 2022, XBB.1.5 made up 75.3% of COVID-19 cases in northeastern states.

Those states include Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island and Vermont, the CDC said.

Even though XBB numbers are currently lower in western parts of the country, Dr. Marvasti of Arizona stressed there's no doubt the subvariant will catch on just about everywhere else.

"It's definitely the majority of cases in the Northeast, and we expect that to be for the whole country," he

said.

"In Arizona, my expectation is that it's going to climb pretty quickly, especially since we have a lot of winter visitors here this time of year, and we're going to have more folks with the Phoenix Open and the Super Bowl," he also said. (The Phoenix Open golf tournament takes place Feb. 6-12, 2023; the Super Bowl is Feb. 12, 2023.)

"It's going to increase in the coming weeks no matter what level it's at right now," he added.

Although it's still too soon to tell how the new strain will impact hospitalization and death rates, neither Siegel nor Marvasti is expecting a steep increase.

Marvasti noted that hospitalizations have been less of an issue since omicron's appearance.

This is because omicron variants are known for attacking the upper respiratory tract — the nose and sinuses — instead of the lower respiratory tract in the lungs, he said.

"Which is one of the reasons why you see less people on ventilators," he explained.

Both experts stressed that even though symptoms may be less severe, people who are at high risk or immunocompromised should continue taking appropriate steps toward prevention, including wearing masks and getting vaccinated.

While keeping up with vaccinations is important, Siegel said, he added that these constantly emerging variants question the efficacy of current vaccines on the market.

The XBB's immuno-evasive properties are "bothering" health experts the most, he noted.

At a recent news briefing, Harvard Medical School assistant professor of medicine Kathryn Stephenson said that even though the original COVID vaccines may have lost some of their punch against new variants, they're still holding up well against severe illness and death.

One possible solution could be incorporating Omicron-updated boosters to further enhance protection, she said.

This would require more research and funding into "better" vaccines such as inhaled vaccinations, said Dr. Siegel.

"My philosophy toward protection from this virus is the more immunity you have, the better," he said.

In an effort for everyone to stay healthy, Dr. Marvasti encouraged practicing other ways to boost immunity, including getting enough sleep, managing stress, reducing inflammation, eating healthier, taking probiotics, staying hydrated and exercising.

"People should recognize that there are a lot of things you can do to help boost immunity and improve your ability to fight off infections including COVID," he said.

Those who've come down with either XBB subvariant can continue treating it as they would any other coronavirus case.

Siegel also recommended the prescription medication Paxlovid as a treatment in some cases, under the guidance of a doctor.

Return to Top

HEADLINE	**01/04 California declares state of emergency**
SOURCE	**https://www.cbsnews.com/news/california-rain-flooding-atmospheric-river/**

GIST	California Gov. Gavin Newsom has declared a state of emergency and drivers are being asked to stay off the roads as a major series of storms carried by an atmospheric river is dropping massive amounts of rain across a wide swath of California from Los Angeles to the Oregon border. Some areas could get more than 10 inches of rain in the next day or so. Meteorologists are warning it could be deadly. In Sacramento County, there's a race to repair breached levees. "If that water comes up real high again, with those kind of flows, we're going to start having trouble," said Leland Schneider, who is with the Cosumnes River Levee District. Roads are flooding throughout Northern California, prompting fears of landslides and power outages. State officials issued a dire warning on Wednesday. "This may be one of the most challenging and impactful series of storms to touch down in California in the last five years," said Nancy Ward, director of the California Governor's Office of Emergency Services. The jet stream stretches across the Pacific, all the way to Indonesia. The amount of water funneling straight into California is up to 15 times the flow at the mouth of the Mississippi River. The ground is already so saturated that any rain can cause immediate flooding. In San Francisco, already battered by record rainfall, the demand for sandbags is so high that the city has exhausted its supply. But the good news is that the storm is bringing more snow to California's Sierra Nevada than in the past decade. The snowpack is vital to the state's water supply, affected by years of drought.
Return to Top	

HEADLINE	**01/04 WHO worried about China Covid surge**
SOURCE	**https://abcnews.go.com/Health/wireStory/worried-surge-covid-china-amid-lack-info-96184640**
GIST	GENEVA -- The head of the World Health Organization said Wednesday the agency is “concerned about the risk to life in China” amid the coronavirus’ explosive spread across the country and the lack of outbreak data from the Chinese government. WHO Director-General Tedros Adhanom Ghebreyesus said the agency recently met with Chinese officials to underline the importance of sharing more details about COVID-19 issues including hospitalization rates and genetic sequences, even as the pandemic continues to recede globally since it began in late 2019. “Data remains essential for WHO to carry out regular, rapid and robust risk assessments of the global situation,” Tedros said at a press briefing. Tedros said he understood why numerous countries have recently taken measures against travelers coming from China, saying “it’s understandable that some countries are taking steps to prevent their citizens” given the void of information about COVID-19. WHO emergencies chief Dr. Michael Ryan said the testing protocols implemented by some countries were not a restriction against travel. “It's not an excessive measure based on individual countries' risk assessment,” Ryan said. He noted that for the past three years, China has had some of the world's harshest rules regarding COVID-19. “The reality for China is that many countries (now feel) they don’t have enough information to base

their risk assessment," he said.

Earlier this week, Chinese officials sharply criticized COVID-19 testing requirements imposed on visitors from China and threatened countermeasures against countries involved, which include the U.S. and several European nations.

"We believe that the entry restrictions adopted by some countries targeting China lack scientific basis, and some excessive practices are even more unacceptable," Foreign Ministry spokesperson Mao Ning said at a briefing Tuesday.

The WHO's Ryan added that there were continuing concerns about how Chinese officials are recording coronavirus deaths, saying that their definition, which only counts COVID-19 deaths if there is a record of respiratory failure, is too narrow.

Throughout December, China recorded only 13 official COVID-19 deaths, despite many thousands of cases every day and reports about overwhelmed hospitals, fever clinics and crematoriums.

A WHO expert group said Wednesday that no worrying new COVID variants have been identified in China based on the information authorities have shared, including genetic sequences deposited into a public database. The WHO said Chinese scientists have now shared more than 770 sequences, with omicron subvariants BA.5 and its descendants accounting for more than 97% of all local infections. Globally, BA.5 variants comprise about 68% of all sequences.

The European Centre for Disease Prevention and Control said it did not expect the surge of COVID-19 in China to affect the outbreak in Europe, given the high rates of vaccination across the continent. It also noted that the variants spreading in China were already present in Europe, suggesting that any spillover from China would have a negligible impact.

Maria Van Kerkhove, the WHO's technical lead on COVID-19, said the agency was currently evaluating the significance of the variant known as XBB.1.5, which has recently comprised an increasing proportion of cases in the U.S.

"Our concern is how transmissible it is," Van Kerkhove said. "The more this virus circulates, the more chances it will have to change," she said, adding that further waves of transmission do not necessarily have to translate into more deaths, with the wide availability of vaccination and drugs.

Van Kerkhove said there is no data yet to prove that XBB.1.5 causes more severe disease, but that the WHO is working on a new risk assessment of the variant that it expects to release soon.

Return to Top

HEADLINE	**01/04 Russia hypersonic missile-armed ship**
SOURCE	**https://abcnews.go.com/International/wireStory/russias-hypersonic-missile-armed-ship-patrol-global-seas-96192661**
GIST	Russian President Vladimir Putin on Wednesday sent a frigate armed with the country's latest Zircon hypersonic missile on a trans-ocean cruise in a show of force as tensions with the West escalate over the war in Ukraine. Russia touts that the Zircon missile can evade any Western air defenses by flying at an astounding 7,000 miles per hour (11,265 km/h). Here is a glance at the ship and its weapons. THE PRIDE OF THE RUSSIAN NAVY Commissioned by the navy in 2018 following long trials, the Admiral Gorshkov is the first ship in the new

series of frigates which were designed to replace the aging Soviet-built destroyers as a key strike component of the Russian navy.

Armed with an array of missiles, the ship is 130-meters (427-feet) long and has a crew of about 200.

In 2019, it circled the world oceans on a 35,000-nautical mile journey.

INTENSIVE TESTS

The Admiral Gorshkov has served as the main testbed for the latest Russian hypersonic missile, Zircon.

In recent years, the Zircon has undergone a series of tests, including being launched at various practice targets. The military declared the tests successful and Zircon officially entered service last fall.

Zircon is intended to arm Russian cruisers, frigates and submarines and could be used against both enemy ships and ground targets. It is one of several hypersonic missiles that Russia has developed.

THE NEW WEAPON

Putin has hailed Zircon as a potent weapon capable of penetrating any existing anti-missile defenses by flying nine times faster than the speed of sound at a range of more than 1,000 kilometers (over 620 miles).

Putin has emphasized that Zircon gives the Russian military a long-range conventional strike capability, allowing it to strike any enemy targets with precision.

Russia's hypersonic weapons drive emerged as the U.S. has been working on its own Conventional Prompt Global Strike capability that envisions hitting an adversary’s strategic targets with precision-guided conventional weapons anywhere in the world within one hour.

Putin heralded Zircon as Russia's answer to that, claiming that the new weapon has no rival, giving Russia a strategic edge.

Months before ordering the invasion of Ukraine, Putin put the U.S. and its NATO allies on notice when he warned that Russian warships armed with Zircon would give Russia a capability to strike the adversary's “decision-making centers” within minutes if deployed in neutral waters.

Speaking via video link during Wednesday's sendoff ceremony, Putin again praised Zircon as a “unique weapon” without an “equivalent for it in any country in the world.”

OTHER RUSSIAN HYPERSONIC WEAPONS

Russia has already commissioned the Avangard hypersonic glide vehicles for some of its ground-based intercontinental ballistic missiles that constitute part of Russia’s strategic nuclear triad. Putin has hailed the Avangard's ability to maneuver at hypersonic speeds on its approach to target, dodging air defenses.

The Russian military has also deployed the Kinzhal hypersonic missiles on its MiG-31 aircraft and used them during the war in Ukraine to strike some priority targets. Kinzhal reportedly has a range of about 1,500 kilometers (about 930 miles).

PATROL DUTY

Russian Defense Minister Sergei Shoigu reported to Putin on Wednesday that the Admiral Gorshkov will patrol the Atlantic and Indian Oceans and the Mediterranean, but didn’t give further details.

Shoigu said the Admiral Gorshkov's crew will focus on “countering the threats to Russia, maintaining regional peace and stability jointly with friendly countries.” He added the crew will practice with

	hypersonic weapons and long-range cruise missiles “in various conditions." Some military experts say a single, hypersonic missile-armed warship is no match for the massive naval forces of the U.S. and its allies. But others noted that the frigate's potential deployment close to U.S. shores could be part of Putin's strategy to up the ante in the Ukrainian conflict. “This is a message to the West that Russia has nuclear-tipped missiles that can easily pierce any missile defenses,” pro-Kremlin political analyst Sergei Markov wrote in a commentary.
Return to Top	

HEADLINE	**01/04 Iran lashes France over new cartoons**
SOURCE	**https://abcnews.go.com/International/wireStory/iran-lashes-france-new-charlie-hebdo-cartoons-96194108**
GIST	DUBAI, United Arab Emirates -- Iran summoned the French ambassador on Wednesday to condemn the publication of offensive caricatures of the country's Supreme Leader Ayatollah Ali Khamenei in the French satirical magazine Charlie Hebdo. The magazine has a long history of publishing vulgar cartoons mocking Islamists, which critics say are deeply insulting to Muslims. Two French-born al-Qaida extremists attacked the newspaper's office in 2015, killing 12 cartoonists, and it has been the target of other attacks over the years. Its latest issue features the winners of a recent cartoon contest in which entrants were asked to draw the most offensive caricatures of Khamenei, who has held Iran's highest office since 1989. The contest was billed as a show of support for anti-government protests rocking Iran. One of the finalists depicts a turbaned cleric reaching for a hangman's noose as he drowns in blood, while another shows Khamenei clinging to a giant throne above the raised fists of protesters. Others depict more vulgar and sexually explicit scenes. Iran’s Foreign Minister Hossein Amirabdollahian vowed a “decisive and effective response” to the publication of the cartoons, which he said had insulted Iran's religious and political authorities. The French government, while defending free speech, has rebuked the privately-owned magazine in the past for fanning tensions. Iran has been gripped by nationwide protests for nearly four months following the death in mid-September of Mahsa Amini, a 22-year-old woman who had been detained by Iran's morality police for allegedly violating the country's strict Islamic dress code. Women have taken the lead in the protests, with many stripping off the compulsory Islamic headscarf in public. The protesters have called for the overthrow of Iran's ruling clerics in one of the biggest challenges to their rule since the 1979 Islamic Revolution that brought them to power. Charlie Hebdo, which has published similarly offensive cartoons about dead child migrants, virus victims, neo-Nazis, popes, Jewish leaders and other public figures, presents itself as an advocate for democracy and free expression. But it routinely pushes the limits of French hate speech laws with often sexually explicit caricatures that target nearly everyone. The paper drew fire for reprinting caricatures of Islam's Prophet Muhammad that were originally published by a Danish magazine in 2005. Those cartoons were seen as sacrilegious and deeply hurtful to Muslims worldwide, many of whom nevertheless condemned the violent response to the drawings.
Return to Top	

HEADLINE	**01/04 Covid surges in Beijing**

SOURCE	https://abcnews.go.com/International/wireStory/beds-run-beijing-hospital-covid-brings-sick-96213821
GIST	BEIJING -- Patients, most of them elderly, are lying on stretchers in hallways and taking oxygen while sitting in wheelchairs as COVID-19 surges in China's capital Beijing. The Chuiyangliu hospital in the city's east was packed with newly arrived patients on Thursday. By midmorning beds had run out, even as ambulances continued to bring those in need. Hard-pressed nurses and doctors rushed to take information and triage the most urgent cases. The surge in severely ill people needing hospital care follows China abandonment of its most severe pandemic restrictions last month after nearly three years of lockdowns, travels bans and school closures that weighed heavily on the economy and prompted street protests not seen since the late 1980s. It also comes as the the European Union on Wednesday "strongly encouraged" its member states to impose pre-departure COVID-19 testing of passengers from China. Over the past week, EU nations have reacted with a variety of restrictions toward travelers from China, disregarding an earlier commitment to act in unity. Italy — where the pandemic first exacted a heavy toll in Europe in early 2020 — was the first EU member to require coronavirus tests for airline passengers coming from China, but France and Spain quickly followed with their own measures. That followed the imposition by the U.S. of a requirement that all passengers from China show a negative test result obtained in the previous 48 hours before departure. China has warned of "countermeasures" if such policies were to be imposed across the bloc. Still, World Health Organization head Tedros Adhanom Ghebreyesus said Wednesday he was concerned about the lack of outbreak data from the Chinese government. China has sought to get more of its elderly population vaccinated, but those efforts have been hampered by past scandals involving fake medications and previous warnings about adverse reactions to the vaccines among older people. China's domestically developed vaccines are also considered less effective than the mRNA jabs used elsewhere.
Return to Top	

Cyber, Tech Awareness

Top of page

HEADLINE	01/04 Wrongly jailed: facial recognition error
SOURCE	https://arstechnica.com/tech-policy/2023/01/facial-recognition-error-led-to-wrongful-arrest-of-black-man-report-says/
GIST	Police in Louisiana reportedly relied on an incorrect facial recognition match to secure warrants to arrest a Black man for thefts he did not commit. Randal Reid, 28, was in jail for almost a week after the false match led to his arrest, according to a report published Monday on NOLA.com, the website of the Times-Picayune/New Orleans Advocate newspaper. Reid told the newspaper that he had never even been to Louisiana: Local police pulled over Reid on Nov. 25 as he drove on Interstate 20 in DeKalb County, Georgia, headed to a late Thanksgiving celebration with his mother, he said. "They told me I had a warrant out of Jefferson Parish. I said, 'What is Jefferson Parish?,'" Reid said. "I

have never been to Louisiana a day in my life. Then they told me it was for theft. So not only have I not been to Louisiana, I also don't steal."

Reid was booked into the DeKalb County jail as a fugitive but was let go on Dec. 1, a jail official said.

Reid's lawyer, Tommy Calogero, said that Jefferson Parish Sheriff's Office detectives "tacitly" admitted the error and rescinded the warrant, the report said. "I think they realized they went out on a limb making an arrest based on a face," Calogero said.

“Police could have checked his height and weight”

Describing his time in jail, Reid said he was "not eating, not sleeping. I'm thinking about these charges. Not doing anything because I don't know what's really going on the whole time. They didn't even try to make the right ID."

The case reportedly began with a June 2022 theft of more than $10,000 worth of Chanel and Louis Vuitton purses in Metairie, Louisiana. Calogero said it wouldn't have been hard to determine that Reid wasn't the culprit, who was reportedly "caught on camera in June entering numbers from a stolen credit card at the register" in the store.

A mole on Reid's face was one of the differences that ultimately forced police to release him, Calogero said. Calogero also "estimated a 40-pound difference between Reid and the purse thief he saw in surveillance footage," the Times-Picayune/New Orleans Advocate report said. The culprit, unlike Reid, had "flabby arms."

"Police could have checked his height and weight or made an effort to speak to him or asked to walk through his house to look for evidence. He would have complied," Calogero told the newspaper.

It's not clear exactly what facial recognition was used in this case. In previous cases, Jefferson Parish Sheriff Joe Lopinto's office requested facial recognition analyses through the Louisiana State Analytic and Fusion Exchange in Baton Rouge, which uses Clearview AI and MorphoTrak systems, the report said.

Clearview software compares faces to pictures on social media and many other sources. "Our platform, powered by facial recognition technology, includes the largest known database of 30+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources," the company's website says.

Sheriff’s office denied newspaper’s request for warrant

The Times-Picayune/New Orleans Advocate report indicates that the wrong facial recognition match led to two warrants for Reid's arrest. The first was obtained by the Jefferson Parish Sheriff's Office, and the second was for a separate crime being investigated by Baton Rouge police.

"A Baton Rouge Police Department detective then adopted JPSO's identification of Reid to secure an arrest warrant alleging he was among three men involved in another luxury purse theft the same week at a shop on Jefferson Highway, court records show," the Times-Picayune/New Orleans Advocate report said.

The report said Lopinto's office did not respond to requests for information and "denied a formal request for the July 18 arrest warrant for Reid and copies of policies or purchases related to facial recognition, citing an ongoing investigation." The separate warrant obtained by Baton Rouge police "does not say how Lopinto's office identified Reid," the report said.

We contacted the Sheriff's office today and will update this article if we get any new information.

Privacy concerns and evidence of bias in facial recognition systems have fueled a movement to ban government use of the technology. "Facial recognition software is particularly bad at recognizing African-Americans and other ethnic minorities, women, and young people, often misidentifying or failing to identify them, disparately impacting certain groups," the Electronic Frontier Foundation says.

Return to Top

HEADLINE	**01/05 Evolving tactics of Vidar stealer**
SOURCE	**https://thehackernews.com/2023/01/the-evolving-tactics-of-vidar-stealer.html**
GIST	The notorious information-stealer known as Vidar is continuing to leverage popular social media services such as TikTok, Telegram, Steam, and Mastodon as an intermediate command-and-control (C2) server. "When a user creates an account on an online platform, a unique account page that can be accessed by anyone is generated," AhnLab Security Emergency Response Center (ASEC) disclosed in a technical analysis published late last month. "Threat actors write identifying characters and the C2 address in parts of this page." In other words, the technique relies on actor-controlled throwaway accounts created on social media to retrieve the C2 address. An advantage to this approach is that should the C2 server be taken down or blocked, the adversary can trivially get around the restrictions by setting up a new server and editing the account pages to allow the previously distributed malware to communicate with the server. Vidar, first identified in 2018, is a commercial off-the-shelf malware that's capable of harvesting a wide range of information from compromised hosts. It typically relies on delivery mechanisms like phishing emails and cracked software for propagation. "After information collection is complete, the extorted information is compressed into a ZIP file, encoded in Base64, and transmitted to the C2 server," ASEC researchers said. What's new in the latest version of the malware (version 56.1) is that the gathered data is encoded prior to exfiltration, a change from the previous variants that have been known to send the compressed file data in plaintext format. "As Vidar uses famous platforms as the intermediary C2, it has a long lifespan," the researchers said. "A threat actor's account created six months ago is still being maintained and continuously updated." The development comes amid recent findings that the malware is being distributed using a variety of methods, including malicious Google Ads and a malware loader dubbed Bumblebee, the latter of which is attributed to a threat actor tracked as Exotic Lily and Projector Libra. Risk consulting firm Kroll, in an analysis published last month, said it discovered an ad for the GIMP open source image editor that, when clicked from the Google search result, redirected the victim to a typosquatted domain hosting the Vidar malware. If anything, the evolution of malware delivery methods in the threat landscape is in part a response to Microsoft's decision to block macros by default in Office files downloaded from the internet since July 2022. This has led to an increase in the abuse of alternative file formats like ISO, VHD, SVG, and XLL in email attachments to bypass Mark of the Web (MotW) protections and evade anti-malware scanning measures. "Disk image files can bypass the MotW feature because when the files inside them are extracted or mounted, MotW is not inherited to the files," ASEC researchers said, detailing a Qakbot campaign that leverages a combination of HTML smuggling and VHD file to launch the malware.
Return to Top	

HEADLINE	**01/04 Healthcare disruptions rise**
SOURCE	**https://www.scmagazine.com/analysis/ransomware/healthcare-disruptions-rise-due-to-ransomware-attacks-**

	though-reporting-gaps-limit-insights
GIST	Ransomware attacks on healthcare delivery organizations doubled between 2016 and 2021, from 43 reported attacks to 91. However, it's likely these numbers and impacts are underestimated due to limited data caused by underreporting, according to a new study published in JAMA Health Forum. One out of five ransomware attacks were not listed in the Department of Health and Human Services Office for Civil Rights database. While these gaps may have been caused by a low amount of compromised protected health information, the researchers noted that it might also be due to "confusion about whether ransomware attacks must be reported through official channels when they involve encryption, but not actual removal, of data from computer systems." HHS previously attempted to clear up this confusion as far back as 2016, after ransomware actors began targeting the healthcare sector in force and found many entities weren't notifying the regulatory body. At that time, they stressed that it was providers who bore the onus for proving data wasn't accessed by the attackers or they must report the incident to HHS. Given the difficulty in finding that evidence, HHS warned that ransomware incidents should be presumed a data breach. But current reporting requirements "lack either an enforcement mechanism or a penalty for noncompliance," the researchers wrote. "Even when an entity reports an attack, there is no sanction for doing so outside of the legislated 60-day window, which may explain the high proportion of ransomware attacks with delayed reporting." These reporting gaps are contributing to the lack of data on ransomware impacts on both care delivery and data exposure. The researchers suggest that instead, legislators should "shape an informed and well-targeted policy response" to strengthen data collection around cyberattacks. **Ransomware's affect on healthcare delivery** Across all sectors in the last year, security researchers struggled to gauge whether ransomware attacks were on the rise or stagnating. What's clear is that attackers are getting smarter and the cost to recover from these attacks is drastically increasing across all sectors — impacting cyber insurance coverage in the process. In healthcare, the impacts of ransomware are readily seen in each hospital attack that have confirmed the patient safety risks posed by these long periods of network downtime. At least three global health systems are currently in downtime after ransomware incidents, which has led to care diversion, appointment cancellations and delays. But as noted in JAMA, there's simply not enough data to fully understand the minutiae of hospital setting impacts after ransomware. While the researchers noted the study's limits, the data does shine a light on incident response and care disruptions. The researchers studied a total of 374 ransomware incidents reported between 2016 and 2021, with documented evidence of care delivery disruptions for 166 of the 374 analyzed attacks. While the data did not show a statistically significant increase in overall operational disruptions, at least 32 of the incidents were tied to disruptions that exceeded over two weeks, 41.7% of which included electronic system downtime. Delays or scheduled care cancellations were seen in 10.2% of the recorded incidents and 4.3% saw ambulance diversion processes. There was also an increase in the share of attacks that involved ambulance diversions. While disruptions varied by the type of organization, hospitals were the most likely to experience a disruption during a ransomware attack.

Further, all ransomware incidents have an organizational effect on system safeguards and the response of leadership. The researchers were able to document "disruptions to care delivery during nearly half of all ransomware attacks, but the scope of the problem is likely larger."

"The most frequent disruption was to electronic systems, which frequently forced a switch to paper charting," according to the report. "These operational disruptions may harm patients, especially those experiencing emergencies and for whom timely treatment is crucial."

Further analysis is needed to "quantify an empirical association between ransomware attacks and patient outcomes."
The data suggests that ransomware attacks on healthcare "organizations have increased in sophistication as well as in frequency," researchers wrote. The "findings represent the only census of ransomware attacks on healthcare delivery organizations."

However, these estimates "of magnitude align with findings in the gray literature, and the trend over time is consistent with reports that ransomware actors increasingly targeted healthcare delivery organizations during the COVID-19 pandemic," they added.

In terms of healthcare targeting, clinics of all specialties were the most common healthcare entity to face a ransomware attack, followed by hospitals, other delivery organization sites, ambulatory surgical centers, behavioral health organizations, dental offices, and post–acute care organizations.

About 53% of all ransomware attacks affected multiple facilities within the attacked organization. Prime examples of multi-site outages brought on by ransomware include Universal Health Services, Scripps Health, CommonSpirit Health, and University of Vermont Health Network.

The ransomware impact on patient data
The data of nearly 42 million patients was compromised by the 374 analyzed ransomware attacks, a more than 11-fold increase from 2016 to 2021.

These impacts held true through 2022, where each of the 15 largest healthcare data breaches affecting more than 1 million patients each, although not all were caused by ransomware.

The report confirmed the evolution of ransomware attacks during the study period. Each year, ransomware became more likely to expose the information of greater numbers of patients, regardless of organization type.

What's more, providers were more likely to report the attacks and data impacts late to HHS. The number of attacks reported more than twice the mandated 60-day "increased substantially in 2020 and 2021." HHS reminded providers of the timely reporting requirement late last year.

Of the 290 incidents reported to HHS, 54.3% were reported outside of the 60-day reporting window.

Although about 1 in 5 healthcare organizations were reportedly able to restore data from backups after a ransomware attack, "the likelihood of healthcare organizations restoring ransomware-encrypted or stolen data from backups decreased" from 2016 to 2021.

Additionally, the researchers found evidence that the ransomware actors made some or all of the stolen protected health information public in 59 of the attacks by posting it on dark web forums. As the years have progressed, it's become increasingly likely for all or some stolen information to be publicly leaked.

While limited, the researchers were able to confirm the increase in frequency and sophistication of ransomware attacks against the healthcare sector from 2016 to 2021. Data confirms the frequent disruptions and exposure of PHI, but more research is needed to "more precisely understand the operational and clinical care consequences of these disruptions."

	As lawmakers seek to address the threat of ransomware across all sectors, the researchers urged "them to focus on the specific needs of healthcare delivery organizations, for which operational disruptions may carry substantial implications for the quality and safety of patient care."
Return to Top	

HEADLINE	**01/05 Play used new method in Rackspace attack**
SOURCE	**https://www.securityweek.com/play-ransomware-group-used-new-exploitation-method-rackspace-attack**
GIST	The recent ransomware attack targeting Rackspace was conducted by a cybercrime group named Play using a new exploitation method, the cloud company revealed this week. **Rackspace told the media** that a previously unknown exploit was used to gain access to its network and steal data. The incident apparently involved a customer's credentials getting compromised, which gave the attackers access to one of its servers on November 29. **The incident** forced Rackspace to **shut down** its Hosted Exchange environment. The company is now in the **process of recovering the data** stored on the impacted Exchange servers. Multiple class action **lawsuits** have been filed against Rackspace in response to the breach and the company's **shares** have been on a downward trend since the incident was disclosed. Cybersecurity researchers **Anis Haboubi** and **Dominic Alvieri** have provided *SecurityWeek* the addresses that point to the Play ransomware operation's Tor-based leak website. There is no mention of Rackspace on the site at the time of writing. Rackspace has not said whether it has paid a ransom to the cybercriminals. The Play ransomware (also known as PlayCrypt) emerged in June 2022. The cybercriminals are deploying file-encrypting malware on compromised systems and stealing data from victims in an effort to increase their chances of getting paid. According to data from deep web intelligence project **DarkFeed**, Play was the sixth most active ransomware operation in December 2022, with 16 new victims announced last month. CrowdStrike reported in December that recent Play ransomware attacks targeting Microsoft Exchange servers had been observed using a new exploit chain that bypassed official mitigations for the flaws tracked as **ProxyNotShell**. The new exploit chain, dubbed **OWASSRF** because it targets Outlook Web Application (OWA), leverages one of the ProxyNotShell vulnerabilities and CVE-2022-41080, an Exchange Server flaw addressed by Microsoft in November 2022, alongside ProxyNotShell. CrowdStrike did not name Rackspace in its blog post, but Rackspace has now confirmed that it's highly confident that exploitation of CVE-2022-41080 was involved in the attack. The individual vulnerabilities exploited in the attack were known and they were patched by Microsoft in November, before the attack on Rackspace, but the way they were chained was new. An external Rackspace advisor revealed that the cloud company had applied ProxyNotShell mitigations in September, when the vulnerabilities came to light, but did not install the November patches due to concerns related to reported operational issues caused by the patches. In addition, Rackspace representatives said Microsoft's **advisory for CVE-2022-41080** did not mention remote code execution. It's worth pointing out, however, that Microsoft did assign the issue an 'exploitation more likely' exploitability rating.
Return to Top	

HEADLINE	**01/05 Slack's GitHub code repositories stolen**
SOURCE	**https://www.bleepingcomputer.com/news/security/slacks-private-github-code-repositories-stolen-over-holidays/**
GIST	Slack suffered a security incident over the holidays affecting some of its private GitHub code repositories. The immensely popular Salesforce-owned IM app is used by an estimated 18 million users at workplaces and digital communities around the world. **Customer data is not affected** BleepingComputer has come across a security incident notice issued by Slack on December 31st, 2022. The incident involves threat actors gaining access to Slack's externally hosted GitHub repositories via a "limited" number of Slack employee tokens that were stolen. While some of Slack's private code repositories were breached, Slack's primary codebase and customer data remains unaffected, according to the company. The wording from the notice [1, 2] published on New Year's eve is as follows: "On December 29, 2022, we were notified of suspicious activity on our GitHub account. Upon investigation, we discovered that a limited number of Slack employee tokens were stolen and misused to gain access to our externally hosted GitHub repository. Our investigation also revealed that the threat actor downloaded private code repositories on December 27. No downloaded repositories contained customer data, means to access customer data, or Slack's primary codebase." Slack has since invalidated the stolen tokens and says it is investigating "potential impact" to customers. At this time, there is no indication that sensitive areas of Slack's environment, including production, were accessed. Out of caution, however, the company has rotated the relevant secrets. "Based on currently available information, the unauthorized access did not result from a vulnerability inherent to Slack. We will continue to investigate and monitor for further exposure," states Slack's security team. **Security update hidden from search engines?** Ironically, the security update speaks of Slack taking your "security, privacy, and *transparency* very seriously," and yet comes with some caveats. For starters, this "news" item doesn't appear on the company's *international* news blog aside other articles, at the time of writing. Additionally, contrary to Slack's earlier blog posts, this update (when accessed in some regions, e.g. UK) is marked with 'noindex'—an HTML feature that is used to exclude a webpage from search engine results, thereby making it harder to discover the page. BleepingComputer further observed that the "meta" tag containing the "noindex" attribute was itself placed towards the bottom within the page's HTML code, in an elongated line that overflows without breaking. This means, those viewing the source code (like us) wouldn't readily get to see the buried tag unless they actively searched (Ctrl+F) the source code for it. Per convention, HTML head and meta tags are typically placed at the top of a page. We noticed though, Google has already indexed the U.S. advisory published without the tag. Other techniques employed by businesses looking to limit the visibility of uncanny news may include the use of geo-fencing and tailoring the robots.txt file. Such techniques, including the use of 'noindex' in important announcements, are typically frowned upon. In some cases, though, 'noindex' attribute may be

	erroneously applied when the aim was to achieve generating 'canonical' links. Last year, infosec reporter and editor Zack Whittaker called out LastPass and GoTo for employing similar tactics with LastPass' 2022 security breach disclosure. In August 2022, Slack reset user passwords after accidentally exposing their password hashes in a separate incident. Unsurprisingly, that particular notice is also marked with a 'noindex' (both the U.S. and international versions). In 2019, Slack announced it had reset passwords for about 1% of users impacted by the 2015 data breach who additionally met a set criteria. The good news, with regards to the most recent security update is that no action needs to be taken by customers, for now.
Return to Top	

HEADLINE	**01/04 Five Guys suffers data breach**
SOURCE	**https://www.darkreading.com/attacks-breaches/five-guys-data-breach-hr-data**
GIST	The Five Guys burger empire has been hit with what appears to be a "smash-and-grab" operation: Cyberattackers busted into a file server and made off with the personally identifiable information (PII) of people who applied to work at the chain. Details are scant, but in a form letter to the impacted sent out on Dec. 29, Five Guys chief operating officer Sam Chamberlain noted that an "unauthorized access to files" was discovered on Sept. 17 and was blocked the same day. He added, "We conducted a careful review of those files and, on December 8, 2022, determined that the files contained information submitted to us in connection with the employment process, including your name and [variable data]." What was that "variable data," one might ask? Turke & Strauss LLP, a law firm that's investigating the matter on behalf of the victims, identifies the information as including Social Security numbers and drivers' license data. Five Guys did not immediately respond to a request for verification or comment from Dark Reading. Five Guys employs about 5,000 people worldwide, according to Forbes, and presumably the turnover and number of applications for open positions is similar to other food-service jobs. But while that means that a large number of people could potentially be affected by the breach, the company has so far left it unclear how many people were actually caught up in the incident. Five Guys also hasn't announced what, if any, shoring up of security it plans to do in the wake of the incident, only noting that it engaged law enforcement and a cybersecurity firm, and that it would provide credit monitoring. Brad Hong, customer success manager at Horizon3ai, notes that improvements to defense should be an important part of the incident response. "An unfortunate precedent has been set [by the infamous Equifax breach] to simply provide credit monitoring, shifting the onus of action back to the consumer instead of the organization announcing the technological steps taken to prevent breaches in the future," he says. **A Whole Menu of Follow-on Attacks** Researchers note that the unfolding situation could prove difficult for both the individual victims and the burger purveyor itself. This isn't Five Guys' first time being flamed on the cybercrime grill, as BullWall executive vice president Steve Hahn notes — and a prior incident illustrates just what could be at stake for both.

"In a past breach of Five Guys, the threat actor used the stolen data to make fraudulent charges on bank debit and credit cards, and one such bank, Trustco, was hit with $100,000 in fraudulent charges from customers of theirs that have been part of this data breach," he tells Dark Reading. "If the bad guys got that much out of Trustco, imagine how much they've bilked from Chase or Bank of America."

As for the impact to the company, Trustco went on to file a lawsuit against Five Guys in New York for damages related to issuing new cards and reimbursing victims for fraudulent charges.

In this more recent case, John Bambenek, principal threat hunter at Netenrich, notes that there are any number of follow-on attacks that threat actors could mount using the data, even if it doesn't include payment-card information.

"The most immediate use of this data is to realize there are a handful of people on the lower end of the economic scale who are looking for jobs," he says. "I imagine there will be scams and mule recruitment lures sent to those people in the near future."

Hahn meanwhile mentions that the craftier cybercriminal types will often also try to take advantage of the fear and reaction in the market when such an incident is publicized, in the form of ultra-believable phishing efforts.

"Victims may get an email: 'We apologize but as you may have heard your data was part of our data breach,'" he explains. "'Please click here to reset your password.' These emails can look identical to emails from Five Guys and they can even spoof the Five Guys domain. Once the user puts in their credentials, they threat actor now has access to all the other sites they use that password on, like PayPal, Amazon, or Venmo."

Jim Morris, chief security adviser at Tanium, also tells Dark Reading that the potential for a cybercrime ripple effect could also include extortion, affecting applicants and organizations alike.

"Any victimized organization could receive double extortion threats — i.e., ask for money to not leak or sell the data," he says. "Individuals whose information is contained in the breach could be victims of triple extortion, whereby the attackers demand money from them to in turn not sell or use their data."

A Smash (& Grab) Burger of Data Theft

Since the data breach notice indicates that the bad guys accessed a single file server, with no lateral movement, this is likely a case of financially motivated attackers looking for low-hanging fruit, researchers say — and finding it.

Restaurants and food-service outlets have a unique set of financial challenges (like razor-thin margins) that can often lead to them deprioritizing security, even as they collect reams of data via online ordering, reservations systems, HR systems, and more, on an order of magnitude that far outstrips other sectors, says Andrew Barratt, vice president at Coalfire.

"The challenge is real — we have adaptive threat actors who will chase down any point of access versus defenders with limited budgets and a whole raft of macro-economic stresses to focus in on too," he says. "Really, we need to keep visibility of these kind of compromises high so that executives don't discount them as 'won't happen to me.'"

Others are less charitable. Horizon3ai's Hong adds, "Unless the attack vector in this incident was a novel one, all signs point to this incident being another example of a company that chose returns over security. With Five Guys pulling in close to $2 billion in revenue, I'd be interested to see what their cybersecurity spend was."

Meanwhile, Web-facing systems could exacerbate the risk, Casey Ellis, founder and CTO at Bugcrowd, says.

	"This sounds a lot like a recruiting system where candidates upload their resumes," he tells Dark Reading. "Having these sorts of systems available to the Internet makes sense when you consider the recruiting and job application process, but if something is more available to a public user, it's also more available to a potential attacker." He adds, "Common Web coding flaws like Indirect Object References (IDOR), authentication flaws, and even injection flaws can enable this type of attacker outcome without the need for lateral movement." Indeed, Tanium's Morris notes that the most common break-in approaches by threat actors looking for easy pickings tend to be the exploitation of known vulnerabilities, and phishing and stolen credentials. As such, there are simple steps that could make bottom-feeding data thieves simply move on to an easier target. "Organizations can combat these attacks by having robust life-cycle management of all computer hardware and software. This requires identifying critical assets and data and protecting them accordingly," he says. "Asset life-cycle management must also include sustainable and efficient vulnerability and patching programs. Additionally, strong authentication and authorization processes that includes multifactor authentication need to be employed."
Return to Top	

HEADLINE	**01/04 Toyota discloses data breach**
SOURCE	**https://gbhackers.com/toyota-discloses-data-breach/?web_view=true**
GIST	Toyota Motor Corporation reveals a data breach that may have compromised the personal information of its customers after an access key was made available to the public on GitHub for over five years. The data breach at Toyota Kirloskar Motor, a joint venture with Indian giant Kirloskar Group, has been reported to the appropriate Indian authorities, according to Toyota India. “Toyota Kirloskar Motor (TKM) has been notified by one of its service providers of an incident that might have exposed the personal information of some of TKM’s customers on the internet”, Toyota Kirloskar Motor (TKM) stated in an email statement. **A Portion of T-Connect Site Source Code Published On GitHub** The carmaker recently learned that some of the source code for its T-Connect website was unintentionally posted on GitHub. The report stated that around 296,000 customer records may have been compromised due to this issue. The company built the T-Connect app, which gives car owners access to the infotainment system of their vehicle and allows them to keep an eye on who has access to it. Along with the code, the data server access key that held client data such as email addresses and management numbers was also included. By a developer subcontractor, the source code was exposed. “In December 2017, the “T-Connect” website development subcontractor mistakenly uploaded part of the source code to their GitHub account while it was set to be public, in violation of the handling rules”, according to the notice published by the company. “This incident was caused by the inappropriate handling of the source code by the development contractor company. We will proceed”. According to the reports, between December 2017 and September 15, 2022, an unauthorized third party might have had access to the information of Toyota consumers. 296,019 clients are affected, the GitHub repository was locked in September 2022, and the keys were modified.

	Although there are no indications of data theft, the Japanese manufacturer comes to the conclusion that it is impossible to completely rule out the possibility that someone may have accessed and stolen the data. "As a result of an investigation by security experts, although we cannot confirm access by a third party based on the access history of the data server where the customer's email address and customer management number are stored; at the same time we cannot completely deny it. We now have." reads the notice published by the company. Notably, the Company declared that it will apologize and notify each affected consumer separately. Toyota has set up a separate form for users to check if their data was exposed on its website. **Lookout for Scams** Users of T-Connect who signed up between July 2017 and September 2022 may be subject to scams and other types of fraud. The company advises customers to be on the lookout for such scams. Here it's possible that spam emails like "spoofing" or "phishing schemes" could be sent using email addresses. "If you receive a suspicious e-mail with an unknown sender or subject, there is a risk of virus infection or unauthorized access, so please do not open the attached file and immediately delete the e-mail itself. Please be careful when accessing the address (URL) described in the email", reads the notice.
Return to Top	

HEADLINE	**01/04 The Guardian suffers ransomware attack**
SOURCE	**https://www.theregister.com/2023/01/04/guardian_ransomware_attack/?&web_view=true**
GIST	Long-standing British newspaper The Guardian has told staff to continue working from home and notified the UK's data privacy watchdog about the security breach following a suspected ransomware attack before Christmas. The publication broke the news about the "serious IT incident" on its systems on December 21, and said the attack affected parts of the company's technology infrastructure. At the time, it told staff to work from home. "We believe this to be a ransomware attack but are continuing to consider all possibilities," The Guardian Media Group Chief Executive Anna Bateson and Editor-in-Chief Katharine Viner told staff last month. Since then, the newspaper has notified Britain's Information Commissioner's Office (ICO) about the breach. "Guardian News and Media has made us aware of an incident and we are making enquiries," an ICO spokesperson told *The Register*. According to the ICO's rules, organizations must notify the government agency within 72 hours of discovering a ransomware attack. Also this week, The Guardian confirmed that most of its staff in the UK, US and Australia will continue working from home until at least January 23. "As we previously announced, the Guardian's systems have been subject to a serious network disruption," a spokesperson told *The Register*. "We have been able to keep publishing our journalism digitally and in print, but a number of key IT systems have been affected. The work to restore our systems fully is ongoing and will take some weeks. We have asked most staff to work from home for the next three weeks to allow our technical teams to focus on essential technical work." The spokesperson declined to answer any additional questions about the security incident. So far, none of the usual suspects have claimed responsibility for the purported ransomware attack.

	However, ransomware gangs including LockBit have been especially busy over the past month, with that group of criminals attacking (and then apologizing for attacking) Canada's largest children's hospital and Los Angeles' public housing authority, among others. At least 219 local governments, health-care providers, colleges, universities and school districts in the US alone were victims of ransomware attacks last year, according to numbers published this week by Emsisoft Malware Lab. The security firm has reportedly similarly high stats in its earlier reports since 2019. "The fact that there seems not to have been any decrease in the number of incidents is concerning," report authors said. Additionally, a report [PDF] by the Financial Crimes Enforcement Network (FinCEN), part of the US Treasury, found that the impact of ransomware attacks — measured in Bank Secrecy Act filings — hit $1.2 billion 2021, up 188 percent compared with 2020.
Return to Top	

HEADLINE	**01/04 December disclosures ransomware victims**
SOURCE	**https://www.techtarget.com/searchsecurity/news/252528876/December-ransomware-disclosures-reveal-high-profile-victims?&web_view=true**
GIST	While the number of ransomware attacks disclosed and reported in December did not increase from the previous month, many victims were high-profile companies such as cloud service provider Rackspace. For the past year, TechTarget Editorial has tracked ransomware incidents against U.S. organizations through public disclosures from the offices of state attorneys general and various media reports. There were 22 confirmed disclosures and public reports in December, compared with 25 in November; however, like past months, the number is likely higher due to ongoing security investigations. The education and public sectors remained popular targets throughout the month, but perhaps the most damaging fallout resulted from an attack against Rackspace on Dec. 2. The attack struck the cloud provider's Hosted Exchange environment, forcing Rackspace to shut down the service and migrate customers to Microsoft 365. Other major enterprises suffered attacks, according to reports and disclosures last month. Chicago-based engineering firm Sargent & Lundy suffered a ransomware attack in October, which CNN confirmed in December. While the company, which has worked with the U.S. Department of Defense and Department of Energy, has not issued a statement, CNN said it obtained a memo that confirmed data belonging to multiple electric utilities was stolen during the intrusion. Another significant attack occurred against Wabtec Corporation in June, but the rail and transportation technology company, which has 27,000 employees around the world, did not report it until Dec. 30. In a statement posted to its website, Wabtec confirmed stolen data was "posted to the threat actor's leak site." Affected information included medical records, health insurance information, financial account information, payment card information, and account usernames and passwords. A December data breach notification by commercial roofing company CentiMark disclosed that it stopped a ransomware attack that occurred in August, but not before threat actors accessed some of its network. Potentially viewed or stolen information included names, dates of birth, Social Security numbers and driver's license numbers. Based in Pennsylvania, the company has more than 95 offices across the U.S., Canada and Mexico. While details into ransomware attacks are often scarce or delayed, two incidents last month offered some insight into recovery efforts and costs.

	On Dec. 1, Little Rock School District (LRSD) in Arkansas confirmed a network issue occurred on Nov. 11. Subsequently, Little Rock KATV reported that the school board voted to pay a $250,000 ransom demand to recover stolen data. However, it appears there was backlash over the district's transparency and how it handled the incident. Greg Adams, LRSD board president, issued a statement to stakeholders on Dec. 15 to address the concerns, citing input from cybersecurity firms and legal teams. "Under the advice of these advisors, we were told to minimize the public messaging regarding the incident, as it could cause drastic and harmful actions by the Threat Actors," Adams wrote in the statement. In addition, Mayor Lori Klein Quinn confirmed the City of Tomball, Texas, was hit by ransomware on Dec. 20, which resulted in an emergency city council meeting on Dec. 30. During the meeting, David Esquivel, city manager, was authorized to spend $50,000 for "recovery of city systems and data," according to a report by Community Impact. As of Jan. 1, Klein Quinn said the city did not have a date for when systems would be fully restored, and the city's network and online services remained down Wednesday. Attacks on the education sector also continued last month. Bristol Community College (BCC) in Massachusetts reported that ransomware encrypted its network on Dec. 23, and as of Wednesday, email and other online services remained unavailable. BCC recommended changing passwords on both professional and personal accounts. Knox College in Illinois also experienced prolonged downtime following a ransomware attack on Nov. 26, which the *Galesburg Register-Mail* publicly disclosed on Dec. 2. In addition, NBC News reported that the threat actors sent ransom demand emails directly to students.
Return to Top	

HEADLINE	**01/04 Critical flaws in popular automaker vehicles**
SOURCE	**https://securityaffairs.com/140328/hacking/bmw-mercedes-toyota-other-carmakers-flaws.html?web_view=true**
GIST	Cybersecurity researcher Sam Curry and his colleagues discovered many vulnerabilities in the vehicles manufactured by tens of carmakers and services implemented by vehicle solutions providers. The vulnerabilities could have been exploited by threat actors to perform a broad range of malicious activities, from unlocking cars to tracking them. The flaws discovered by the experts affected vehicles of popular brands, including Kia, Honda, Infiniti, Nissan, Acura, Mercedes-Benz, Genesis, BMW, Rolls Royce, Ferrari, Ford, Porsche, Toyota, Jaguar, Land Rover. The research team also discovered flaws in the services provided by Reviver, SiriusXM, and Spireon. The exploitation of some flaws gave the experts access to hundreds of Mercedes mission-critical internal applications via improperly configured SSO. An attacker could have also exploited them to achieve remote code execution on multiple systems. The flaws also allowed attackers to access to the content of the memory of some systems, leading to the exposure of Mercedes' employee/customer PII. In the case of BMW and Rolls Royce, experts found SSO vulnerabilities which allowed them to access any employee application as any employee. The experts were able to access to internal dealer portals and retrieve sales documents for BMW by providing VIN numbers. The experts were also able to access any application locked behind SSO on behalf of any employee, including applications used by remote workers and dealerships. *"While testing BMW assets, we identified a custom SSO portal for employees and contractors of BMW. This was super interesting to us, as any vulnerabilities identified here could potentially allow an attacker to compromise any account connected to all of BMWs assets. For instance, if a dealer wanted to access*

	the dealer portal at a physical BMW dealership, they would have to authenticate through this portal. Additionally, this SSO portal was used to access internal tools and related devops infrastructure." reads the analysis published by Curry. "To demonstrate the impact of the vulnerability, we simply Googled "BMW dealer portal" and used our account to access the dealer portal used by sales associates working at physical BMW and Rolls Royce dealerships." Experts were also able to achieve a full vehicle takeover on Kia via deprecated dealer portal Some of the vulnerabilities discovered by the experts allowed the researchers to retrieve owner information, including the physical address, in other cases the flaws allowed tracking vehicles. *"Ability to send retrieve vehicle location, send vehicle commands, and retrieve customer information via vulnerabilities affecting the vehicle Telematics service" reads the analysis related to the issues impacting Porsche.* The experts also demonstrated how to exploit some flaws to access the Reviver license plate service and update any vehicle status to "STOLEN" which updates the license plate and informs the authorities. The good news is that all the flaws discovered by the experts were addressed by the carmakers and service providers.
Return to Top	

HEADLINE	**01/04 Cops hacked thousands of phones: legal?**
SOURCE	**https://www.wired.com/story/encrochat-phone-police-hacking-encryption-drugs/**
GIST	**FOR A WEEK** in October 2020, Christian Lödden's potential clients wanted to talk about only one thing. Every person whom the German criminal defense lawyer spoke to had been using the encrypted phone network EncroChat and was worried their devices had been hacked, potentially exposing crimes they may have committed. "I had 20 meetings like this," Lödden says. "Then I realized—oh my gosh—the flood is coming." Months earlier, police across Europe, led by French and Dutch forces, revealed they had compromised the EncroChat network. Malware the police secretly planted into the encrypted system siphoned off more than 100 million messages, laying bare the inner workings of the criminal underground. People openly talked about drug deals, organized kidnappings, planned murders, and worse. The hack, one of the largest ever conducted by police, was an intelligence gold mine—with hundreds arrested, homes raided, and thousands of kilograms of drugs seized. But it was just the beginning. Fast-forward two years, and thousands of EncroChat users across Europe—including in the UK, Germany, France, and the Netherlands—are in jail. However, a growing number of legal challenges are questioning the hacking operation. Lawyers claim investigations are flawed and that the hacked messages should not be used as evidence in court, saying rules around data-sharing were broken and the secrecy of the hacking means suspects haven't had fair trials. Toward the end of 2022, a case in Germany was sent to Europe's highest court. If successful, the challenge could potentially undermine the convictions of criminals around Europe. And experts say the fallout has implications for end-to-end encryption around the world. "Even bad people have rights in our jurisdictions because we are so proud of our rule of law," Lödden says. "We're not defending criminals or defending crimes. We are defending the rights of accused people." **Hacking EncroChat** Around 60,000 people were signed up to the EncroChat phone network, which was founded in 2016, when it was busted by cops. Subscribers paid thousands of dollars to use a customized Android phone that could, according to EncroChat's company website, "guarantee anonymity." The phone's security features included encrypted chats, notes, and phone calls, using a version of the Signal protocol, as well as the ability to "panic wipe" everything on the phone, and live customer support. Its camera, microphone, and GPS chip could all be removed.

Police who hacked the phone network didn't appear to break its encryption but instead compromised the EncroChat servers in Roubaix, France, and ultimately pushed malware to devices. While little is known about how the hacking took place or the type of malware used, 32,477 of EncroChat's 66,134 users were impacted in 122 countries, according to court documents. Documents obtained by Motherboard showed all data on the phones could potentially be hoovered up by the investigators. This data was shared between law enforcement agencies involved in the investigation. (EncroChat has claimed it was a legitimate company and shut itself down after the hack.)

Across Europe, legal challenges are building up. In many countries, courts have ruled that messages from EncroChat can be used as evidence. However, these decisions are now being disputed. The cases, many of which have been reported in detail by Computer Weekly, are complex: Each country has its own legal system with separate rules around the types of evidence that can be used and the processes prosecutors need to follow. For instance, the UK largely doesn't allow "intercepted" evidence to be used in court; meanwhile, Germany has a high bar for allowing malware to be installed on a phone.

The most high-profile challenge so far comes from lawyers in Germany. In October, a regional court in Berlin sent an EncroChat appeal to the Court of Justice of the European Union (CJEU), one of the continent's highest courts. The judge asked the court to make decisions on 14 points about how the data was transferred across Europe and how it was being used in criminal cases. The Berlin court highlighted the secretive nature of the investigation. "Technical details on the function of the trojan software and the storage, assignment, and filtering of the data by the French authorities and Europol are not known," a machine-translated version of the court ruling says. "The functioning of the trojan software is fundamentally subject to French military secrecy."

Lödden, who is not involved in the case that has reached the CJEU but is coordinating with around a dozen other lawyers involved in European EncroChat cases, says people were offered good deals by judges and took reduced sentences for pleading guilty in some of the first cases he worked on. Since then, he has used several lines of defense. His challenges often involve questioning what legal basis was used to justify capturing the data from people's devices. Another approach involves questioning the data itself. "You don't know how the French got the data," he says. "The only thing that is clear is that it's not the full data, because there are gaps, and the data they got is not fully decrypted."

There is no set date for the European Court to review the case; although in another high-profile legal challenge, two British EncroChat users have taken their case to Europe's top human rights court. However, a French case, which is set to be decided this month, could make a difference to other cases across Europe. In October, the French Court of Cassation questioned previous EncroChat legal decisions and said they should be re-examined. "The judge who authorized this measure was not in charge of 60,000 investigations, but only one, and therefore ordered a disproportionate act," say lawyers Robin Binsard and Guillaume Martine, who are challenging the collection of the data. "We have to defend our clients without knowing how the investigators acted," they say.

Despite the legal challenges, police forces across Europe have lauded the EncroChat hack and how it has helped put criminals in jail. When the hack was announced in June 2020, hundreds of people were arrested in huge coordinated policing operations. Police in the Netherlands discovered shipping containers that were being used as "torture chambers" by criminals.

Since then, there has been a stream of EncroChat cases reaching courts and people being jailed for some of the most serious crimes. The data from EncroChat has been a real boon to law enforcement—organized crime arrests in Germany soared by 17 percent following the police busts, and at least 2,800 people have been arrested in the UK.

Cases in the UK have seen two men who planned a revenge shooting sentenced to 18 years in jail each, a drug dealer jailed for 14 years for supplying 8 kilograms of cocaine and heroin, and six men jailed for a combined 140 years after plotting to smuggle ecstasy internationally inside the arm of a digger. And in June last year, police in the Dominican Republic reportedly arrested the alleged masterminds behind the

EncroChat system itself.

France's National Gendarmerie military police, the UK's National Crime Agency, and Germany's federal investigative police agency, Bundeskriminalamt, declined to comment on the ongoing legal cases. Jan Op Gen Oorth, a spokesperson for Europol, says the investigation was conducted as part of a joint investigation team that involved multiple EU bodies and national police forces. "The data in the case was captured on the basis of the provisions of French law and with judicial authorization, through the frameworks for international judicial and law enforcement cooperation," Oorth says.

Encryption Fights

EncroChat isn't the only encrypted phone network police have hacked or dismantled. Law enforcement operations against Ennetcom, Sky ECC, and Anom—the FBI covertly took over the latter and ran the network—highlight broader tensions around encryption. For years, police have complained that encryption stops them from accessing data, while at the same time having multiple alternative ways to get around encryption. In Europe and the US, laws are being proposed that could weaken encryption as the technology becomes the default.

Breaking phone networks billed as encrypted and highly secure—some may be legitimate, while others are shadier—raises questions about law enforcement tactics and transparency. "What we're seeing is that policing authorities and law enforcement authorities are effectively normalizing a policing practice that sets a really dangerous precedent in terms of surveillance," says Laure Baudrihaye-Gérard, the legal director for Europe of criminal justice nonprofit Fair Trials.

Adam Jackson and Cerian Griffiths, law professors at the UK's Northumbria University who have been analyzing EncroChat legal issues, say there is a "judicial appetite" to use the collected data to convict criminals, but that the correct processes must be followed, as more cases like this may happen in the future. "You want bad people to be prosecuted for the seriously bad things that they're going to do," they say. "You just want to make sure that it's done properly, in a way that is evidentially sound. And that means that they don't get appeals down the line that undermine those convictions."

One court in Finland has already ruled that data gathered by the FBI from Anom couldn't be used—the severity of the alleged crimes did not justify the way the data was accessed, local reports claimed. Meanwhile, Italy's Supreme Court has said the methods used to access Sky ECC messages should be disclosed.

More than 100 Dutch lawyers have warned that the lack of transparency around the hacks could create a slippery slope. In the future, the lawyers wrote in an open letter, Signal or WhatsApp could be targeted. "These services are also already placed in a suspicious corner or are likely to get there, while that suspicion is only based on the use of strong encryption and the protection of one's own privacy."

Jessica Shurson, a lecturer in law at the University of Sussex and a former US prosecutor, says the hacking cases should be included in broader debates about the importance of encryption for people's security. "They're finding ways to access encrypted systems, through hacking, through their own malware," Shurson says. "Can we really say that law enforcement is 'going dark' because of encrypted data when we see these cases coming up every couple of years showing that, actually, they can access the encrypted systems?"

Return to Top

HEADLINE	**01/04 Internet access inequities Seattle, Portland**
SOURCE	**https://crosscut.com/equity/2023/01/study-reveals-internet-access-inequities-seattle-and-portland**
GIST	CenturyLink customers in Seattle and Portland receive wide-ranging levels of service for the same price, with poorer residents and people of color more likely to be burdened by slow speeds, according to a new analysis of digital inequities in U.S. cities. Seattle had the worst disparities among cities examined in the Pacific Northwest. About half of its lower-income areas were offered slow internet service, compared to just 19% of upper-income areas.

Addresses in neighborhoods with more residents of color were also offered slow internet more frequently: 32.8% of them, compared to 18.7% of areas with more white residents.

CenturyLink offerings in Portland were also uneven, as 27% of addresses in lower-income areas were offered speeds below the federal broadband standard of 25 mbps, compared with 16% of higher-income areas. In both Portland and Seattle, neighborhoods rated "hazardous" to mortgage lenders in mid-20th century "redlining" maps — which were used to discriminate against minority communities — were more likely to see the worst internet deals in both cities today.

The disparities in the Pacific Northwest's two largest cities were revealed in a national investigation this fall by The Markup, a nonprofit news outlet covering technology's impacts on society, which showed that four major internet service providers routinely offer slower speeds to some neighborhoods for the same price as higher speeds offered to other areas. The Markup analyzed service offers from CenturyLink, Verizon, AT&T and EarthLink at more than 800,000 addresses in the largest cities in 38 states.

The Markup found income-related disparities in Seattle, Portland and 17 other cities. In two-thirds of the cities where the news outlet had sufficient data to compare, the worst deals were offered to the least-white neighborhoods.

In addition to Seattle and Portland, the worst offers in 20 other cities aligned with former redlining boundaries.

A spokesperson for Lumen, CenturyLink's parent company, denied discriminatory intent and criticized The Markup's investigation in a statement.

"The methodology used for the report you read is deeply flawed," said Mark Molzen in an email. "We do not engage in discriminatory practices like redlining and find the accusation offensive. While we can't comment on behalf of other providers, we can say we do not enable services based on any consideration of race or ethnicity."

Comcast, the primary internet service provider for both Seattle and Portland, was not included in the analysis because it doesn't offer different speeds for the same price, a practice known as "tier flattening." EarthLink also serves Seattle and Portland, but the analysis did not show evidence of income or race-related disparities.

Local and state officials in Oregon and Washington expressed concern but little surprise at the inconsistencies unearthed in the analysis.

"I don't doubt at all that disparities exist in Portland," said Rebecca Gibbons, strategic initiatives manager for Portland's Office of Community Technology.

While Comcast and one or two other providers also serve the cities, the new data reaffirm that lower-income residents are stuck with the worst options, Gibbons told InvestigateWest.

"If a consumer has only one option, they're beholden to that customer service level, those fees, those rates," she said. "We would like it to be as competitive as possible."

Oregon Rep. Pam Marsh, D-Southern Jackson County, who sits on Oregon's Joint Committee on Information Management and Technology, said the findings showed "clearly a calculated business decision as to who will pay them for the services."

"The result is, people are left out," she said.

Tier flattening isn't illegal. Although policymakers at all levels agree broadband is an essential tool for social, economic and educational empowerment, it isn't regulated as a utility, like electricity. Providers

can set their own prices, and local and state authorities can't force them to build modernized infrastructure in areas that might be less profitable.

While advocates and government officials see an opportunity to offer additional input during the allocation of $65 billion in federal funding approved in the 2021 Infrastructure Investment and Jobs Act, the money may not yield much relief for underserved urban neighborhoods.

Francella Ochillo, executive director of Next Century Cities, a national nonprofit that advocates for reliable and affordable high-speed internet for all, said The Markup's analysis of providers shines a light on the plight of underserved residents.

"Companies have very robust communications staffers and lobbyists to make sure they convince people you are not seeing what you see with your own eyes, but we do see it with our own eyes," Ochillo said. "And we actually have the numbers to prove it."

But looking at data is just a first step, she said.

"We've set up a system where unequal outcomes are guaranteed," she said. "If we want to have a different result, we're going to not only have to examine but dismantle some of the practices that got us here."

Neighborhoods left behind

The stories of CenturyLink's expansion into Portland and Seattle closely mirror each other.

In 2015, the landline company began looking to compete in the high-speed internet market with cable companies like Comcast, which controlled the bulk of it. CenturyLink sought cable franchises and permits, and began building out its high-speed internet and cable infrastructure, officials said.

Just a few years into its expansion in Seattle and Portland, however, CenturyLink's appetite for expansion as a cable provider flagged, officials said. Gibbons said CenturyLink pulled out of the Portland market in 2020, and the company left the Seattle cable market in 2021, according to a spokesperson for the mayor's office.

CenturyLink remained an active internet service provider, but when it stopped expanding as a cable provider, Gibbons said, "our regulatory authority to require them to build out into every neighborhood went away."

As a result, CenturyLink's rollout into both cities has led to some pretty lopsided scenarios.

In Portland, for example, two blocks north of the Lloyd Center on Broadway Street, CenturyLink offers an office building internet speeds of up to 15 megabits per second for $50 a month. A mile and a half southeast, in the upper-income Laurelhurst area, residents of a house on 35th Avenue could pay $20 less per month for 200 megabits per second — a lower price for speeds more than 13 times as fast.

During its time as an internet service provider, CenturyLink has run afoul of the Washington and Oregon attorneys general over complaints about confusing and duplicate charges. In 2020, lawsuits resulted in a $6 million payout in Washington and a $4 million settlement in Oregon.

A spokesperson with the Oregon Department of Justice said the issue of tier flattening doesn't seem to violate Oregon's Unfair Trade Practices Act, and no cases have been brought against a broadband provider under that law.

State officials and advocates acknowledged practical factors contributing to the disparities. Building out infrastructure is expensive, and businesses choose to do it in areas where they think they can make a profit on the costs.

But, Ochillo said, “Involuntary exclusion has a discriminatory impact, whether or not it’s what you intended.

“Communities know when their students can’t go to school online, when their small businesses don’t operate with the same type of resilience, when they don’t have the same type of telehealth options as other people.”

Lots of money, few regulations

Internet service providers, or ISPs, also point to their participation in the Affordable Connectivity Program as proof of their commitment to advancing digital equity.

The federal program, which launched in 2021 to replace an older broadband program, subsidizes internet for lower-income households to the tune of $30 a month, or $75 for households on Indian reservations. Many different indicators of economic need can qualify a household for participation in the program, which is managed by the Federal Communications Commission.

Enrollment is low. Data from mid-2022 show only 27% of eligible households in Portland and Seattle have signed up for the program.

Officials offered a few reasons why that might be. Marsh, the Oregon state representative, criticized the program for being too dependent on ISPs also participating, and Gibbons called the registration requirements “way too burdensome.”

Some aspects of the Infrastructure Investment and Jobs Act indicate that the federal government is beginning to pay attention to how it can more actively tackle digital inequities.

For the first time, the FCC in March began soliciting comments on digital discrimination and equity including “how to implement provisions in the Infrastructure Investment and Jobs Act that require the FCC to combat digital discrimination, and to promote equal access to broadband across the country, regardless of income level, ethnicity, race, religion or national origin.”

The Infrastructure Act funding also allows states and localities new opportunities to weigh in before funding is allocated.

In late November, the FCC published its latest broadband map. It is the primary resource the National Telecommunications and Information Administration, the executive branch office tasked with allocating funding, will use to make decisions. The map is based on self-reported data from the ISPs.

“From what we've seen in the maps, they are dramatically overstating what their true coverage is,” said Evan Marwell, CEO of EducationSuperHighway, a digital equity advocacy nonprofit.

From now through January, the FCC is accepting challenges from states to fine-tune the maps. The Washington Department of Commerce and the Oregon Broadband Office have circulated news releases requesting public input on the FCC maps, including information on how to submit challenges.

But there is a caveat for Portland and Seattle: Despite the billions of dollars flowing, most officials expressed doubt that urban residents will see much of it.

That’s because Congress required states to first spend the Infrastructure Act money on areas that are “unserved,” or considered not to have broadband access at all. Neighborhoods where an ISP already provides service, however limited, won’t likely be touched until the rural, remote areas are taken care of first.

It’s a sore point for city and state officials.

“Yes, rural communities where there’s absolutely no access — we need to be prioritizing them,”

	Gibbons said. “But when you look at the numbers of communities and are using an equity lens, your Black, Indigenous people of color, people with disabilities, the majority of them live in urban communities.” Ochillo said federal policy shifts are needed for widespread change. “The ISPs mentioned in the report get a ton of government subsidies,” she said. “If we know they are getting ... public funds, why aren’t we setting up systems where they have to be accountable to the public?” Instead, she said, “We’ve set up a system where unequal outcomes are guaranteed.”
Return to Top	

HEADLINE	**01/04 Twitter leak: records of 235M accounts**
SOURCE	**https://www.washingtonpost.com/technology/2023/01/04/witter-leak-emails-handles/**
GIST	Records of 235 million Twitter accounts and the email addresses used to register them have been posted to an online hacking forum, setting the stage for anonymous handles to be linked to real-world identities. That poses threats of exposure, arrest or violence against people who used Twitter to criticize governments or powerful individuals, and it could open up others to extortion, security experts said. Hackers could also use the email addresses to attempt to reset passwords and take control of accounts, especially those not protected by two-factor authentication. “This database is going to be used by hackers, political hacktivists and of course governments to harm our privacy even further,” said Alon Gal, co-founder of the Israeli security company Hudson Rock, who spotted the posting on a popular underground marketplace. The records were probably compiled in late 2021, using a flaw in Twitter’s system that allowed outsiders who already had an email address or phone number to find any account that had shared that information with Twitter. Those lookups could be automated to check an unlimited list of emails or phone numbers. Twitter said in August that it had learned of the vulnerability in January 2022 through its reward program for bug reports and that the vulnerability had been accidentally introduced in a code update seven months before that. In July, hackers were spotted selling a set of 5.4 million Twitter account handles and associated emails and phone numbers, which Twitter said was the first it learned that someone had taken advantage of the flaw. The much larger data dump was almost certainly compiled in the same way and has been offered for private sale and circulated for a while before the recent publication, Gal said. Ireland’s Data Protection Commission said last month that it was investigating the earlier breach and that Europe’s General Data Protection Regulation might have been violated. The new batch is likely to add to the intensity of that probe and an ongoing inquiry by the U.S. Federal Trade Commission into whether Twitter has been violating consent decrees in which it promised to better protect user data. The FTC declined to comment. Three-quarters of Twitter users live outside the United States and Canada. Twitter did not respond to an email seeking comment and asking if the company had any advice for users. Those users at the least risk provided throwaway email addresses or ones not tied to them elsewhere.

	But even they could be subject to account takeover attempts, phishing or emailed threats. In its previous statement, Twitter said it fixed the flaw when it learned of it but did not say how long the process took. The report from January 2022 came during a chaotic month when the company fired both of its top security officers. One of them, Peiter Zatko, had been arguing internally that Twitter was grossly unprepared to fend off hacking attempts, and he later filed a formal whistleblower complaint with the Securities and Exchange Commission and testified about the deficiencies in Congress. While 235 million published records ranks among the largest breaches anywhere, it is only the latest in a stretch of security disasters at Twitter dating back more than a decade. Frequent account takeovers led to a 2011 settlement with the FTC that Zatko said the company has been violating. While Elon Musk previously used Zatko's testimony about poor security practices in a failed attempt to get out of buying the company, he has since laid off many of its security staffers.
Return to Top	

HEADLINE	**01/04 US moves to seize FTX digital accounts**
SOURCE	**https://www.wsj.com/articles/judge-ordered-seizure-of-money-from-ftx-digital-markets-accounts-at-silvergate-11672866368?mod=hp_lead_pos3**
GIST	Federal authorities are moving to seize hundreds of millions of dollars in assets in the U.S. tied to the bankrupt cryptocurrency exchange FTX, a sign that the battle over control of the company's remaining funds is escalating. Seth Shapiro, a Justice Department official, said at an FTX bankruptcy court hearing Wednesday that the federal government has seized or is in the process of seizing Robinhood shares whose ownership is disputed by FTX and BlockFi, a cryptocurrency lender that collapsed in late November. The Wall Street Journal previously reported that the dispute involves 56 million shares. "We either believe these assets aren't property of the bankruptcy estate," or fall under some bankruptcy code exception, Mr. Shapiro told Judge John Dorsey on Wednesday in the U.S. Bankruptcy Court in Wilmington, Del. Separately, Katharine Parker, a federal magistrate judge in New York, in December ordered the seizure of money that an FTX unit was keeping in accounts at Silvergate Capital Corp., according to a court filing Wednesday. An earlier court filing put the amount at about $93 million. The Justice Department has accused FTX co-founder Sam Bankman-Fried of stealing billions of dollars of customer money. The U.S. attorney for the Southern District of New York said Tuesday that his office had formed an FTX task force, and that one of its goals is to trace and recover victim assets. The Federal Bureau of Investigation has also filed an affidavit with a New York federal court in order to seize FTX funds. Meanwhile, court-appointed liquidators in the Bahamas have been attempting to recover remaining funds inside bank accounts in the U.S., some of which have been frozen following the crypto exchange's collapse. However, federal authorities have preempted some of that dispute and seized at least some of the disputed funds as their criminal probe of FTX and Mr. Bankman-Fried has widened. The federal government's entrance into a matrix of competing claims for control over FTX assets will likely complicate customers' ability to recover their money, which has been out of reach since November. FTX lawyer James Bromley said during Wednesday's hearing that the seizures were ordered by the

	court in connection with the criminal case in the Southern District of New York involving Mr. Bankman-Fried. He pleaded not guilty to charges of fraud this week. "The question as to the ownership of those Robinhood shares was an open question before the seizure took place," Mr. Bromley said. "We wanted to make sure that it was clear the Robinhood shares that were being seized were being seized from accounts" that aren't currently under the direct control of the bankrupt FTX. Silvergate on Wednesday filed a copy of Judge Parker's warrant that led to the seizure of FTX's funds at the bank. The bank made the filing to a federal bankruptcy court in Delaware handling the insolvency of FTX Digital Markets, a Bahamas-based subsidiary of FTX that housed the company's international exchange. Bahamian regulators placed FTX Digital Markets into liquidation in November, just before FTX's new chief executive, John J. Ray III, placed about 100 FTX subsidiaries under chapter 11 protection in the U.S. FTX Digital Markets' liquidators, appointed by the Supreme Court of the Bahamas, had previously asked to transfer $93 million out of Silvergate and another roughly $50 million held at Moonstone Bank in Washington state into accounts they control. "It would be irresponsible to leave significant U.S. assets (more than $140 million) in the hands of two small crypto banks," the liquidators wrote last month. They pointed to Silvergate being the subject of at least four class-action lawsuits brought by FTX creditors and Silvergate shareholders since November. Silvergate said that the liquidators could have asked for consensual access instead of attempting to obtain it through a court order. "Silvergate, having repeatedly confirmed that the accounts had been frozen, vigorously disputes the implications that the funds are, in any way, at risk of loss," the bank wrote. Authorities' seizure of FTX funds raises questions about how, or if, customers can expect to recover their money locked on the crypto platform. Mr. Ray told Congress in December that FTX's U.S. entity isn't solvent, putting into doubt whether American customers can expect to see their funds returned. He also noted that FTX's international customers' funds were commingled with accounts belonging to Alameda Research, whose own losses on bad crypto bets total in the billions, he said. "We believe we have rights with respect to those assets that can be dealt with later," FTX's Mr. Bromley said of the seized assets. "We are in alignment at the present time with the U.S. government and the law enforcement officials in taking these steps." Mr. Shapiro of the Justice Department said the government would file a notice of seizure so the court is aware of what has been seized by the U.S. government.
Return to Top	

HEADLINE	**01/05 Anonymous: Serbia is 'Putin's puppet'**
SOURCE	**https://www.foxnews.com/world/anonymous-claims-serbia-putins-puppet-russia-expand-war-europe-distract-west**
GIST	Hacking collective Anonymous has accused Serbian President Aleksandar Vucic of acting as "Putin's puppet" as Serbia stirs up conflict with Kosovo in an act that Russia hopes may distract the West from Ukraine. "Russia is trying to open a new front in Europe to distract the West," Ivana Stradner, an adviser to the Foundation for Defense of Democracies' Barish Center for Media Integrity, told Fox News Digital. "Russia does not want to send troops or tanks or jets in the Balkans where Kosovo and Serbia are located,"

Stradner said. "What Russia wants to do [is] create chaos inside the region, so the United States and our allies, so we do not pay attention that much to Ukraine and Russia, you know, to be distracted with what's going on in Kosovo."

Kosovo last week closed its border with Serbia as the two nations face increasing tensions. Ethnic Serbs had set up barricades at the border to protest the arrest of an ex-policeman suspected of being involved in attacks against ethnic Albanian police officers, France 24 reported.

"Such an illegal blockade has prevented the free movement and circulation of people and goods, therefore we invite our citizens and compatriots to use other border points for circulation," Kosovo police said in a statement.

Several shooting incidents followed, with attacks on Kosovar police and international peacekeepers. Serbian armed forces went on heightened alert, but Vucic appeared to ease tensions after reaching an agreement on Dec. 29 that would see the blockade removed, the BBC reported.

Alexander Botsan-Kharchenko, Russian ambassador to Serbia, said Serbia may rely on Russia regarding the Kosovo situation, "regardless of the serious challenges … in the context of the confrontation with NATO," according to Russian news agency TASS.

"We continue to take part in settling current international crises, including in Kosovo," Botsan-Kharchenko said. "We will continue close coordination with Belgrade in defending Serbia's legal rights concerning Kosovo and Metohija."

Kosovo declared its independence from Serbia in 2008, but Serbia has never recognized it and has actively encouraged the country's ethnic Serbian population to defy Kosovar authority.

This potentially chaotic situation presented a prime opportunity for Russian President Vladimir Putin, who treats Serbia as a "very close ally," according to Stradner.

"[Serbia] does not border Russia, but in every possible sense they are supporting Russia when it comes to the war in Ukraine," she said, adding that the Russian ambassador "received extra instructions from Moscow on how to proceed" on the issue.

Despite the removal of the blockade, Anonymous called out Vucic and accused him of prompting the blockade at Putin's request, eventually declaring war on Vucic.

In the first week of the invasion of Ukraine, Russia attacked Ukraine's government websites. The use of cyberattacks prompted Anonymous to declare war on Russia and start targeting Russian websites and commence a series of "hack and dump" attacks.

The large impact of the attacks has seen a large volume of information dumped out in public, including the release of 120,000 Russian soldiers' personal details, access to the Kremlin's CCTV system, and also gas pipelines out of Russia, according to the AnonymousTV Twitter account (it should be noted that Anonymous, by nature, has no single "official" account).

Recent attacks have hit more selective targets such as SIBUR, Russia's largest petrochemical company, and a claim that Vucic is "Mr. Putin's puppet."

"It has come to our attention that the tensions and military provocations in the north of Kosovo by Serbian criminal elements are trying to cause armed conflict," the group said in a video posted to Twitter. "Serbian autocrat President Aleksandar Vucic, a puppet of Vladimir Putin, is trying to destabilize the region using war criminal Slobodan Milosevic's mechanisms of violence and terror, but it is known that this effort will be suicidal for him."

The threat made little dent on Vucic, who responded by posting a picture of himself playing with his dogs

	on Instagram with the message: "We are getting ready for the fight against Anonymous." The group fired back, saying, "#Anonymous is not a small group of powerless people to ignore, we are an organized, globally active, collective of like-minded individuals and our message will be clear, if you don't stop your dangerous actions in #Kosovo," a post on AnonymousTV's Twitter read. Dustin Carmack, a research fellow for cybersecurity, intelligence and emerging technologies at the Heritage Foundation, cautioned that while such revelations may have good intentions, it's hard to predict the knock-on effects. "You saw that throughout different intelligence revelations over the last decade and the impacts that can have in Europe and other places," Carmack told Fox News Digital. "I think it's very difficult in the environment that we are in for anybody to judge – especially a hacktivist group that may have a slim picture of something they think is revealing on one end, even if it is … to know it may affect second-hand or third-hand," Carmack continued. "I think [in] this context, you don't know the nature of Anonymous and who is making that decision." "You don't know what the final tie-in for that person is who makes that decision, and that makes it very difficult for the Brits or Americans or anybody," he added. Fox News Digital sent requests for comment to the Serbian foreign ministry and the U.S. State Department.
Return to Top	

HEADLINE	**01/04 Hack halts Martinique search for new flag**
SOURCE	**https://abcnews.go.com/International/wireStory/cyberattack-halts-martiniques-search-new-flag-hymn-96188729**
GIST	SAN JUAN, Puerto Rico -- A quest to select the first official flag and hymn for the French Caribbean island of Martinique was interrupted Wednesday by a cyberattack. The attack on government servers upended a nearly two-week online voting window that began on Jan. 2. Officials said the attack was not successful but forced them to temporarily shut down the system. They did not say when voting would resume. Residents on the island of more than 370,000 inhabitants had been given 19 flag options and four hymns from which to choose. The island does not have its own official flag and instead uses the French flag at government buildings, although independent activists favor a red, green and black flag. The attack comes less than two months after hackers launched a large-scale cyberattack on government servers in the neighboring French Caribbean island of Guadeloupe.
Return to Top	

Terrorism, Extremism

Top of page

HEADLINE	**01/03 USAO: 'this is a crime of terrorism'**
SOURCE	**https://www.thenewstribune.com/news/local/article270725017.html**
GIST	Two men charged in the Christmas Day attacks on four Pierce County substations, which knocked out power for thousands, appeared in U.S. District Court in Tacoma for the first time on Tuesday following their holiday weekend arrests. Matthew Greenwood, 32, and Jeremy Crahan, 40, both of Puyallup, each face up to 20 years on a charge of conspiracy to damage energy facilities. Greenwood faces an additional charge of possessing

	unregistered firearms, carrying a penalty of up to 10 years in prison, because law enforcement seized two unregistered, short-barrel guns from his residence. "This is a crime of terrorism," assistant U.S. attorney Stephen Hobbs said in court Tuesday. Federal and local law enforcement arrested Greenwood and Crahan on Dec. 31 and booked them into the Federal Detention Center at SeaTac following multiple days of FBI surveillance. Chief Magistrate Judge Richard Creatura will decide during upcoming hearings whether the defendants should be held without bail pending trial at the request of federal prosecutors, who cited an anti-terrorism measure and the risk the defendants could flee or obstruct the case outside custody. Creatura ordered federal public defenders to be assigned to represent the defendants based on their finances. Lance Hester of Tacoma-based Hester Law Group is representing Crahan because the Office of the Federal Public Defender can't represent two co-defendants. Assistant federal public defender Rebecca Fish represented Greenwood on Tuesday. More than 15,000 Puget Sound Energy and Tacoma Power customers lost power early Christmas morning following attacks on substations in South Hill, Elk Plain and Graham, according to charging papers. Damages at the latter two facilities, both owned by Tacoma Power, could cost nearly $3 million and take three years to fix. After his arrest on Saturday, Greenwood told investigators he and Crahan planned the power disruptions to aid a burglary, according to charging papers. Greenwood said they broke into a local business affected by the power outage and stole from the cash register. The men also are suspected of damaging a Puget Sound Energy substation in Kapowsin later in the evening on Christmas, according to charging papers. Court records for Greenwood and Crahan show multiple convictions related to fraud, theft and burglary in Pierce County but no histories of violent crime. Public records also showed a Roy address for Crahan and an eviction proceeding against Greenwood in Graham. Both men will appear in court together on Jan. 17 after Creatura gives a pretrial detention ruling.
Return to Top	

HEADLINE	**01/04 Group alliance threatens Pakistan leaders**
SOURCE	**https://www.voanews.com/a/group-threatens-terror-attacks-on-pakistan-political-leaders/6903743.html**
GIST	A banned alliance of militant groups waging terrorism in Pakistan threatened Wednesday that it would unleash attacks on the country's political leadership for declaring war on the outfit to allegedly "appease" the United States. The Tehrik-e-Taliban Pakistan (TTP), also known as the Pakistani Taliban, issued the warning explicitly to the leaders of the two major partners in the ruling coalition, the Pakistan Muslim League-Nawaz (PML-N) and the Pakistan Peoples Party (PPP). The PML-N is headed by Prime Minister Shahbaz Sharif and the PPP by Foreign Minister Bilawal Bhutto Zardari. The TTP, listed as a global terrorist organization by the U.S. and the United Nations at large, has lately carried out almost daily attacks, killing hundreds of Pakistani security forces and civilians. The militant warning came after Sharif chaired a meeting Monday of the National Security Committee (NSC), the country's highest security-related forum comprising political and military leadership and vowed that terrorism "will be dealt with full force of the state." Pakistani officials say the TTP, an offshoot and ally of Afghanistan's ruling Islamist Taliban, has unleashed its recent wave of terrorist attacks from across the Afghan side of the border. The NSC meeting

	also issued a subtle warning to Taliban rulers, saying “no country will be allowed to provide sanctuaries and facilitation to terrorists.” On Tuesday, a U.S. State Department spokesperson backed Pakistan’s renewed resolve against terrorism and again urged the Afghan Taliban to deliver on their counterterrorism pledges. “The Pakistani people have suffered tremendously from terrorist attacks. Pakistan has a right to defend itself from terrorism,” Ned Price told reporters in Washington. “We continue to call on the Taliban to uphold the very commitment they have made to see to it that Afghan soil is never again used as a launchpad for international terrorist attacks,” he said. “These are among the very commitments that the Taliban have been unable or unwilling to fulfill to date,” Price said. Pakistani Defense Minister Khawaja Asif said this week that Afghanistan harbored an "overwhelming presence” of TTP members. “We have been requesting the Taliban ever since they returned to power (in Kabul) to stop the TTP from plotting terrorist activities in Pakistan,” Asif told local media Monday. He said Islamabad hopes the rulers in Kabul would help rein in the terrorists. A spokesman for the Taliban administration Tuesday rejected Pakistani allegations as “false” and “regrettable.” Zabihullah Mujahid said that his government, which is yet to be given legitimacy by the world, wants peaceful relations with all neighboring countries, including Pakistan, to promote Afghan as well as regional peace and stability. The Taliban reclaimed power in August 2021 as U.S.-led troops withdrew from Afghanistan after 20 years of involvement in war. TTP chief Noor Wali Mehsud and commanders have taken refuge on the Afghan side of the border after fleeing counterterrorism military operations in Pakistan. Officials in Islamabad say the militants have been roaming freely in Afghanistan and directing cross-border terrorism with greater freedom since the Taliban takeover.
Return to Top	

HEADLINE	**01/05 Taliban: anti-terror raids target IS militants**
SOURCE	**https://www.voanews.com/a/taliban-anti-terror-raids-kill-11-islamic-state-group-militants/6905315.html**
GIST	ISLAMABAD — Afghanistan’s Taliban said Thursday their special forces had killed 11 Islamic State group operatives and captured seven others in overnight raids against the group’s hideouts in Kabul and elsewhere in the country. Taliban spokesman Zabihullah Mujahid claimed in a statement the militants had played a central role in organizing recent attacks in the Afghan capital, including a deadly raid on a hotel housing Chinese nationals, an armed attack on Pakistan’s embassy and a suicide bombing of the city military airport. “The security forces’ action destroyed three Daesh shelters in Kabul and Zaranj,” Mujahid said, referring to the capital of southeastern Nimroze province, while providing details of Wednesday’s raids. He used an Arabic acronym for Islamic State’s Afghan chapter, known as IS-Khorasan. “Foreign Daesh members were also among the dead,” Mujahid added, noting the network of militants was also involved in transferring foreign IS-Khorasan members to Afghanistan. “A large quantity of small arms, hand grenades, mines, suicide vests and explosives were seized by security forces. A number of suspects were also taken into custody for further investigation,” he said.

	VOA could not independently verify the claims. The Taliban spokesman said a separate overnight raid in eastern Nangarhar province, which borders Pakistan, resulted in the killing of three IS-Khorasan operatives, including an important commander. The December 12 attack on Kabul's Longan hotel killed or wounded several Taliban forces, while China confirmed five of its nationals had also suffered injuries. Pakistan said the December 2 attack on Islamabad's embassy in the Afghan capital was aimed at assassinating Ubaid ur Rehman Nizamani, the chief Pakistani diplomat in the country. Nizamani escaped unharmed in the shooting incident, but his Pakistani security guard was injured. IS-Khorasan claimed responsibility for both attacks. The group also took credit for plotting last Sunday's deadly suicide bombing of the military airport, claiming it was carried out by a fighter who had participated and survived the raid on the hotel where Chinese nationals were staying. The militant group posted on Telegram that the airport attack killed 20 people and wounded 30 others. Taliban officials disputed those figures but have not shared official casualty toll to date. The repeated attacks in Kabul and elsewhere in Afghanistan have raised questions about claims that Taliban security forces have degraded the presence of IS-Khorasan in the country. Last week, a car bomb in the northeastern Badakhshan border province killed the Taliban regional police chief and his two guards. IS-Khorasan took responsibility for plotting that attack in the provincial capital, Fayzabad.
Return to Top	

HEADLINE	**01/04 DHS: domestic extremism southern border**
SOURCE	**https://abc7chicago.com/domestic-extremism-at-southern-border-could-rise-amid-possible-end-/12654384/**
GIST	Extremist violence targeting migrants along the southwest border could rise amid the possible lifting of the public health restriction known as Title 42, according to a Department of Homeland Security intelligence assessment obtained by ABC News. The bulletin, dated Dec. 23 and issued by DHS' intelligence and analysis branch, came just before the Supreme Court announced that they would hear arguments on whether or not the policy should continue. The high court ordered the controversial restriction, which allows for the rapid expulsion of migrants and is officially intended to prevent the spread of COVID-19, be kept in place until they decide on an appeal from 19 states who want to preserve the policy. The justices will hear the appeal in February. "We assess that the potential for domestic violent extremist (DVE) violence along the US Southwest Border likely will increase in the coming weeks based on recent online calls for violence in response to the anticipated lifting of US Code Title 42," the late-December bulletin states. In particular, the bulletin cites "calls for attacks targeting primarily migrants and critical infrastructure." "But our insight into DVE plotting is constrained by these individuals' use of online security measures to limit exposure to law enforcement," the DHS assessment notes. On social media, the department says extremists have also posted "online calls for violence targeting migrants at the US Southwest Border."

	"The tactics discussed are consistent with DVE messaging and include firearms attacks, the placement of land mines along migration routes, and luring migrants into trailers to poison them with gas, according to DHS reporting," the bulletin states. DHS believes that domestic extremists will be influenced by "perceptions of ... law enforcement action along the border" after Title 42 ends: "This includes perceptions about individuals, groups, or other organizations operating along the border, the treatment of migrants encountered there, and the number of migrants entering the United States." According to the department, social media users have discussed shooting electrical substations near the southern border as a way to "disrupt immigration facilities and public safety and emergency services, judging from DHS reporting." This tactic, the department says, is new and similar to what occurred in early December at a substation in Moore County, North Carolina. Militia extremists pose the greatest threat to law enforcement, the bulletin states, because of their readiness and preparedness. In years past, extremists have targeted immigrant communities, such as in the 2019 mass shooting of an El Paso, Texas, Walmart. "Since at least 2018, DVEs responsible for mass casualty attacks tied to immigration grievances have prioritized soft targets perceived as being densely populated by immigrants or facilitating migration to the United States," the bulletin states.
Return to Top	

HEADLINE	**01/04 DA: machete suspect wanted jihad on cops**
SOURCE	**https://www.seattletimes.com/nation-world/nation/da-times-square-machete-suspect-wanted-jihad-on-police/**
GIST	NEW YORK (AP) — A man accused of attacking police with a machete near New York's Times Square on New Year's Eve was intent on committing a jihad against government officials and shouted "Allahu akbar" before striking one officer in the head and attempting to grab another officer's gun, prosecutors said Wednesday. Trevor Bickford, who was shot by police during the confrontation, was arraigned by video from a Manhattan hospital and ordered to be held without bail. He did not enter a plea and has another court appearance scheduled for Friday. Bickford, 19, of Wells, Maine, is charged with attempting to murder police officers, assault and attempted assault. If convicted, he faces a mandatory life sentence. The attack, at the edge of the high-security zone where throngs of revelers gathered, left three officers injured. Assistant Manhattan District Attorney Lucy Nicholas said Bickford "specifically traveled to New York from Maine in order to begin carrying out his crimes of murder of government officials," arriving in the city a few days before the attack. Bickford had an Amtrak ticket to Miami and wanted to travel abroad, "but then decided to come to New York first in order to kill people and carry out jihad," Nicholas said. He had no known ties to the city or state, she said. Nicholas said Bickford told investigators that "all government officials" were a target for him because of the U.S.'s support of Israel, including police officers, but that he purposely spared civilians from harm. Authorities have been investigating whether Bickford was motivated by Islamic extremism. The Legal Aid Society, a public defender organization representing Bickford, urged the public "to refrain from drawing hasty conclusions and to respect the privacy of our client's family." The machete attack happened about two hours before midnight on Saturday, just outside the area where

people are screened for weapons before gaining entry to one of the world's biggest and most famous New Year's celebrations.

Three officers were struck with the machete before an officer shot the suspect, authorities said. One officer suffered a fractured skull and another had a bad cut. All were expected to recover. Investigators believe the attacker acted alone.

Bickford's mother contacted the Wells, Maine, Police Department on Dec. 10 to express concerns about her son, and the department notified the FBI, Wells Police Capt. Jerry Congdon said Tuesday. He could not discuss the interaction further, but said Bickford was not a concern to local police.

The Times Square attack "was as much of a surprise to us as it was anyone else," Congdon said. "He was certainly flying under the radar."

FBI agents were seen Sunday entering Bickford's family home in Wells, a popular beach destination close to the New Hampshire border. Bickford competed in sports in high school, was part of Maine's state champion wrestling team in 2020 and made the honor roll for his studies at least one year.

Bickford's online postings included some mentions of Islamic extremist views, according to a law enforcement official familiar with the matter. The official could not publicly discuss details about the ongoing investigation and spoke to the AP on condition of anonymity.

In Bickford's criminal complaint, a detective with the FBI's Joint Terrorism Task Force said he told her: "I wanted to kill an officer in uniform."

According to the detective, Bickford said he waited until he saw an officer alone, said "Allahu akbar," walked up to him and hit him over the head with the machete, which he said was a kukri — a machete-like blade with South Asian origins. In Arabic, "Allahu akbar" means "God is great."

According to the detective, Bickford said he then charged another officer, dropped the knife and attempted to grab that officer's gun. Nicholas said Bickford told investigators he wanted to kill the officers with the gun, but couldn't get it out of the holster.

Return to Top

HEADLINE	**01/04 Far-left extremist groups in the US**
SOURCE	**https://www.homelandsecuritynewswire.com/dr20230104-farleft-extremist-groups-in-the-united-states**
GIST	Far-left extremism in the United States was most active during the period between the 1960s and 1980s. In the 1990s, a new type of left-extremism began to emerge – what the FBI calls "special-interest extremism," as expressed by groups such as the Animal Liberation Front (ALF) and Earth Liberation Front (ELF). The Counter Extremism Project (CEP) has released a detailed report which profiles eleven far-left movements either previously or currently active in the United States. Here is the report's Executive Summary: **Executive Summary** Far-left extremism in the United States largely centers around the notion of correcting an injustice but is otherwise broad in its ideological catchment. In the 20th century, U.S. left-wing extremism was synonymous with either communism or causes such as environmentalism. In the 1960s and '70s, the Weather Underground declared war against the U.S. government and carried out a campaign of political violence.(1) According to the FBI, far-left extremism in the United States was most active during the period between the 1960s and 1980s. Special-interest extremism began to emerge on the far-left in the 1990s, resulting in the promulgation of groups such as the Animal Liberation Front (ALF) and Earth Liberation Front (ELF). The FBI estimated that between 1996 and 2002, these two groups were responsible for 600 criminal acts in the United States that caused more than $42 million in damages.(2) Throughout the 1990s and early 2000s, ALF and ELF targeted animal research facilities and corporations for acts of vandalism and destruction of property. After the September 11, 2001, terrorist attacks,

the U.S. government reevaluated how it approached terrorism abroad and at home. While the government focused on al-Qaeda as the primary foreign threat, federal authorities—partly in response to government lobbying by corporations victimized by ecoterrorists—considered ALF and ELF to be the primary domestic terrorism threat in what media dubbed the Green Scare.(3) By 2010, however, federal authorities had shifted their domestic focus to the threat of the far right, which continued to overshadow the radical far left in violent attacks while ALF and ELF focused on property damage.(4)

A July 2020 report by the Center for Strategic and International Studies (CSIS) reviewed almost 900 politically motivated attacks since 1994. Researchers found that far-left attacks had resulted in only one fatality in that 25- year span, compared with 329 fatalities in attacks by the far right.(5) In recent years, however, the radical far left has seen a resurgence in response to the rise of the far right, particularly since the 2017 Unite the Right rally in Charlottesville, Virginia, when far-right protesters clashed with far-left counter-protesters. A revitalized American far left has emerged to lead protest movements against the far right and perceived injustices. Armed groups such as the John Brown Gun Club formed to directly confront the violent far right and a broad interpretation of fascism, which often include symbols of capitalism and corporations. These manifestations have been on display during 2020 protests against police brutality, during which the far left have become increasingly visible and destructive, leading then-President Donald Trump in May 2020 to call for designating the broad anti-fascist ideology Antifa a terrorist organization.(6)

The image of armed leftist groups such as the John Brown Gun Club can also invoke concern. In November 2020, counterinsurgency and military strategy expert David Kilcullen told Salon that while groups such as Redneck Revolt and the John Brown Gun Club claim to be largely defensive and seek to protect people on the streets from violence, the fear they evoke can also be a trigger for violence.(7) This can spark conflict with police or violent far-right groups seeking an excuse to strike a blow to the far left.(8)

The president's desire to label Antifa a terrorist organization highlighted the problematic nature of modern far-left groups in the United States, which are largely less organized than their predecessors. During the mid- to late 20th century, far-left groups dedicated to causes such as Puerto Rican independence carried out bombings and other violent attacks across the United States. By the 1990s, however, authorities had largely dismantled the leadership infrastructure of these groups.(9) Today, the far left largely coalesces around ideologies and not specific individuals or structured organizations. Antifa and black bloc, for example, are centered around a broad opposition to fascism but are otherwise left open for individual interpretation, which results in varying tactics and even beliefs among adherents who may disagree on what is included under the fascist label. There are multiple groups in the United States that affiliate with the Antifa ideology, but they have no formal organizational relationship, formal leadership structure, or shared tactical approach. Similarly, black bloc is primarily a tactic used by far-left protesters rather than an actual group. But because of the tendency for black bloc agitators to dress all in black, including helmets, they draw more attention.

The far left encompasses multiple ideologies, but security experts believe that a large percentage of far-left radicals subscribe to at least one of three main classifications: anarchism, communism/socialism/Marxism, and autonomous radicals.(10) Far-left groups have largely embraced social justice as a raison d'être in protest of perceived restrictions on liberty by the state. In the early and mid-20th century, the Communist Party USA (CPUSA) played a subversive role in promoting communism in the United States and aligned itself with the Soviet Union. Today, CPUSA promotes its dedication to human rights and personal liberties alongside communism, which it heralds as the only guarantor of those freedoms.(11)

Combined with a desire for violent confrontation and rejection of state authority, some on the far left have used social justice issues such as racial equality and immigration rights as a pretext to engage in violent retribution against symbols of the state. This is most prominently seen today in the use of black bloc tactics during protests, which ideological opponents have seized on to cast black bloc and Antifa as organized and unified groups. Anarchist groups such as the Youth Liberation Front are more organized on a local level but have no cohesive national network linking chapters across the country.(12) With the May 2022 leak of a U.S. Supreme Court decision to overturn the 1973 Roe v. Wade decision, which established

the constitutional right to abortion, a new autonomous network emerged called Jane's Revenge. Named after the Jane Collective, an underground organization in Chicago that helped women obtain abortions prior to the 1973 decision, the anonymous network has claimed responsibility for vandalism and attacks on anti-abortion clinics around the United States since May 2022. (13) Online communiques from the network cite a history of extremist violence against abortion clinics forcing the adoption of extreme tactics to maintain their bodily autonomy.(14) Like ALF and ELF, the members of Jane's Revenge justify their extremism as the pursuit of the greater good.

Anarchism is a millennia-old philosophy that advocates a stateless society.(15) French writer Pierre-Joseph Proudhon was the first to label himself an anarchist in 1840.(16) Today's anarchists often cite modern anarchist writer Alfredo M. Bonanno as an inspiration. In his 1977 essay "Armed Joy," Bonanno exhorted followers to "shoot the policeman, the judge, the boss…."(17) Bonanno's works derided capitalism and encouraged followers to tear down its symbols.(18) In his 1993 essay "For An Antiauthoritarian Insurrectionalist International," Bonanno wrote that conservative voices had sidelined the radical left, causing it to regress. In response, Bonanno called for Mediterranean groups to coordinate an anti-authoritarian insurrection.(19)

The far left has not uniformly embraced anarchism. A common theme between anarchist and non-anarchist groups, however, is a rejection of authority. This manifests itself as opposition to colonialism, authoritarianism, and—in common with anarchism— state authority. The far left opposes state oppression and believes that strengthening government and security institutions is a path toward a police state or fascism, which should be confronted.(20) According to German authorities, the extreme left believes that it can goad the state into revealing its true fascist nature by eliciting violent reactions.(21) Far-left protesters have also engaged in violence against the far right as part of a self-declared opposition to racism and fascism, as can be seen by Antifa and black bloc actions during 2020 protests. According to Germany's Bundesamt für Verfassungsschutz, however, the extreme left only superficially opposes fascist movements, focusing more on undermining the capitalist system.(22) U.S. Attorney General William Barr has directly accused Antifa and related groups of hijacking peaceful protests in the United States to promote anarchism.(23)

_____

1 Arthur M. Eckstein, "How the Weather Underground Failed at Revolution and Still Changed the World," Time, November 2, 2016, http://time.com/4549409/the-weather-underground-bad-moon-rising/.
2 Testimony of Dale L. Watson, Executive Assistant Director, Counterterrorism/Counterintelligence Division Federal Bureau of Investigation, Before the Senate Select Committee on Intelligence, Washington, DC, FBI, February 6, 2002, https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-co….
3 Alleen Brown, "The Green Scare," Intercept, March 23, 2019, https://theintercept.com/2019/03/23/ecoterrorism-fbi-animal-rights/; Juliet Eilperin, "As eco-terrorism wanes, governments still target activist groups seen as threat," Washington Post, March 10, 2012, https://www.washingtonpost.com/national/health-science/as-eco-terrorism-… Testimony of Dale L. Watson, Executive Assistant Director, Counterterrorism/Counterintelligence Division Federal Bureau of Investigation, Before the Senate Select Committee on Intelligence, Washington, DC, FBI, February 6, 2002, https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-confronting-theunited-states.
4 Kristina Davis, "Ecoterror arsons unsolved 10 years later," San Diego Union-Tribune, September 14, 2013, https://www.sandiegouniontribune.com/news/public-safety/sdut-ecoterror-a… htmlstory.html; Alleen Brown, "The Green Scare," Intercept, March 23, 2019, https://theintercept.com/2019/03/23/ecoterrorism-fbi-animal-rights/.
5 Lois Beckett, "Anti-fascists linked to zero murders in the US in 25 years," Guardian (London), July 27, 2020, https://www.theguardian.com/world/2020/jul/27/us-rightwing-extremists-at….
6 "Antifa: Trump says group will be designated 'terrorist organization,'" BBC News, May 31, 2020, https://www.bbc.com/news/world-us-canada-52868295.
7 Chauncey Devega, "Doomsday? Nearly half of "strong Republicans" believe it's almost time for armed violence," Salon, July 27, 2022, https://www.salon.com/2022/07/27/doomsday-nearly-half-of-strongrepublicans-believe-its-almost-time-for-armed-violence/.
8 Jason Lange, "U.S. Capitol riot to try to make then-President Donald Trump look bad," Reuters, June 9, 2022, https://www.reuters.com/world/us/half-us-republicans-believe-left-led-jan-6-violence-

	reutersipsos2022-06-09/. 9 Testimony of Dale L. Watson, Executive Assistant Director, Counterterrorism/Counterintelligence Division Federal Bureau of Investigation, Before the Senate Select Committee on Intelligence, Washington, DC, FBI, February 6, 2002, https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-confronting-theunited-states. 10 Jefferson Chase, "After G20: A look at left-wing radicalism in Europe," Deutsche Welle, July 10, 2017, https://www.dw.com/en/after-g20-a-look-at-left-wing-radicalism-in-europe…. 11 "CPUSA Program," Communist Party USA, April 13, 2020, https://www.cpusa.org/party_info/partyprogram/#Capitalism. 12 "About," PNW Youth Liberation Front, accessed September 21, 2020, https://pnwylf.noblogs.org/about/. 13 Judith Levine, "Beyond Revenge, What Does Jane's Revenge Want?," Intercept, June 16, 2022, https://theintercept.com/2022/06/16/janes-revenge-abortion-rights/; Alice Reid, "Report: Group claims credit for Madison anti-abortion office attack, warns of more," NBC 26, May 11, 2022, https://www.nbc26.com/news/state/report-group-claims-credit-for-madison-…. 14 Robert Evans, Twitter post, May 10, 2022, 3:24 a.m., https://twitter.com/IwriteOK/status/1523926941572550656. 15 Kory Flowers, "Understanding the Black Bloc," Police Magazine, January 30, 2015, http://www.policemag.com/channel/patrol/articles/2015/01/understanding-the-black-bloc.aspx. 16 Arif Dirlik, George Woodcock, Franklin Rosemont, and Martin A. Miller, "Anarchism," Encyclopaedia Britannica, accessed November 19, 2018, https://www.britannica.com/topic/anarchism. 17 Alfredo M. Bonanno, "Armed Joy," The Anarchist Library, accessed November 19, 2018, https://theanarchistlibrary.org/library/alfredo-m-bonanno-armed-joy. 18 Alfredo M. Bonanno, "Armed Joy," The Anarchist Library, accessed November 19, 2018, https://theanarchistlibrary.org/library/alfredo-m-bonanno-armed-joy. 19 Alfredo M. Bonanno, "For An Anti-authoritarian Insurrectionalist International," The Anarchist Library, accessed November 19, 2018, http://theanarchistlibrary.org/library/alfredo-m-bonanno-for-an-antiauth…. 20 "Left-wing extremists' fields of activity," Bundesamt für Verfassungsschutz, accessed August 20, 2018, https://www.verfassungsschutz.de/en/fields-of-work/left-wing-extremism/figures-and-facts-left-wingextremism/left-wing-extremists-fields-of-activity-2014. 21 "Brief summary 2017 Report on the Protection of the Constitution," Bundesamt für Verfassungsschutz, 2017, 20, https://www.verfassungsschutz.de/embed/annual-report-2017-summary.pdf 22 "Left-wing extremists' fields of activity," Bundesamt für Verfassungsschutz, accessed August 20, 2018, https://www.verfassungsschutz.de/en/fields-of-work/left-wing-extremism/figures-and-facts-left-wingextremism/left-wing-extremists-fields-of-activity-2014. 23 Claire Hansen, "White House Addresses Trump Pledge to Designate Antifa a Terrorist Group," U.S. News & World Report, June 1, 2020, https://www.usnews.com/news/national-news/articles/2020-06- 01/white-house-addresses-trump-pledge-to-designate-antifa-a-terrorist-group.
Return to Top	

Suspicious, Unusual

Top of page

HEADLINE	**01/05 UK's hottest-ever year in 2022**
SOURCE	**https://apnews.com/article/weather-climate-and-environment-european-union-europe-252cbc366a76291f18b5081ae0b9f18b**
GIST	LONDON (AP) — Britain had its warmest year on record in 2022, official figures showed Thursday, the latest evidence that climate change is transforming Europe's weather. The Met Office weather agency said the provisional annual average temperature in the U.K. was 10.03 degrees Celsius (50 Fahrenheit), the highest since comparable records began in 1884. The previous record was 9.88 Celsius (49.8 Fahrenheit) set in 2014. Met Office scientists said human activity — primarily fossil fuel emissions — has made such warm

	conditions vastly more likely. "The results showed that recording 10C in a natural climate would occur around once every 500 years, whereas in our current climate it could be as frequently as once every three to four years," said Met Office climate attribution scientist Nikos Christidis. Britain is not alone. France's average temperature was above 14 Celsius (57.2 Fahrenheit) in 2022, making it the hottest year since weather readings began in 1900. In Spain, preliminary data from the end of December indicated that 2022 was the hottest year since records started in 1961. Last year saw summer drought and heat waves across much of Europe, with the temperature in Britain rising above 40 degrees Celsius (104 Fahrenheit) for the first time on record. Norway's Svalbard islands in the Arctic had their warmest summer in more than a century of record-keeping. The archipelago's average temperature for June, July and August was 7.4 Celsius (45.3 Fahrenheit), the Norwegian Meteorological Institute said. Autumn brought more heavy rain in parts of Europe, including the mountainous Italian island of Ischia, where downpours in November triggered a massive landslide that pushed cars and buildings into the sea and killed at least a dozen people. Unlike the U.S. and Canada, which have been hit by bitter cold and snowstorms, much of Europe is experiencing unseasonably warm winter weather. In Germany, the year ended with the warmest New Year's Eve on record, with temperatures reaching 20 Celsius (68 Fahrenheit) in the south of the country. Belarus, Belgium, Czechia, Latvia, Poland and the Netherlands all set national record daily highs for Dec. 31 or Jan. 1. As 2023 begins, many low and medium-altitude ski resorts in the Alps, the Pyrenees and other European ranges are suffering from a lack of snow. In Bosnia, spring-like weather has foiled even artificial snow -- either it's too warm to make it, or it melts soon after being spit out onto the slopes. Along the slopes in Bjelasnica near Sarajevo on Wednesday, snow accumulation amounted to little more than several white patches on an otherwise grassy landscape of brown and green.
Return to Top	

HEADLINE	**01/04 World's largest dam water level record low**
SOURCE	**https://www.washingtonpost.com/weather/2023/01/04/kariba-dam-record-low-power-cuts/**
GIST	The water level at the world's largest man-made dam — which generates hydroelectric power for millions of people in Zambia and Zimbabwe — has dropped to a record low, forcing local energy companies to make drastic cuts. The cuts mean no electricity for large portions of the day in these countries, adversely affecting the region's economy and way of life for its residents. The Kariba Dam regulates the flow of water into the Zambezi River, which straddles the border between the two countries, from Lake Kariba, which is formed by the dam. But because of a lack of rainfall and low inflow from the upstream portion of the river and its tributaries, Lake Kariba's water level fell below 1 percent of capacity on Dec. 28, compared with 20 percent one year earlier, according to data from the Zambezi River Authority. The dam generally produces 1,080 megawatts of electricity output for Zambia and 1,050 megawatts to Zimbabwe. Now, both countries are limited to less than 400 megawatts. Zambia's leading power company, ZESCO, which supplies energy to over 80 percent of the country, said

	early Wednesday that it would immediately increase the length of power cuts from six hours to 12 hours. In a statement, ZESCO said that, as of Dec. 31, the water level was at 475.60 meters above sea level, "a situation that has necessitated the reduction of generation." It added that the reduction, to below 400 megawatts, affected "the ability to meet the system load/customer power demand, especially during morning and evening peak demand periods." Because of the insufficient levels, Zimbabweans have been forced to endure 19 hours of power outages a day. The shortage is bringing challenges for small businesses and households that can't afford alternative electricity supplies and rely on hydroelectric power for their daily activities. "Everyone in Zambia now is nervous about the shortage of electricity due to the load shedding being implemented currently by ZESCO," Archie Mulunda, a civil rights activist based in Kitwe, Zambia, told The Washington Post. He worries that power outages will cause food to spoil in supermarkets and that other small businesses will be "seriously affected." He fears that the outages will make it nearly impossible to use his desktop computer, affecting his ability to work from home. Mulunda, 40, is also nervous about what the extended power outages will mean for his wife and three children, who will be home until the middle of January because of school break. "We [will] need to find other means of energy to prepare some warm foodstuff for my children. We really need enough energy for the family use," Mulunda said. "We are more worried about food storage in our homes. Definitely, a lot of people's foodstuff will go bad due to long hours of load shedding." Bloomberg News reported the low water levels have seriously harmed the local fishing industry. Harry Verhoeven, a senior research scholar at Columbia's Center on Global Energy Policy, wrote that the power cuts have already "crippled" Zimbabwe's basic industrial and agricultural activities. "[T]he drying up of the Kariba reservoir has devastating consequences not only for electricity generation and regional water security, but also because it undercuts traditional strategies in Zambia and Zimbabwe for adapting to climate variability," Verhoeven wrote. The dam, which is 420 feet tall and 1,900 feet across and built in the 1950s, may get a boost if the rainy season — which typically extends into March — delivers. However, rains have proved unreliable in recent years. A 2021 study in the Frontiers in Climate journal noted temperatures in Zimbabwe have risen about 1 degree Celsius over the last 40 years, while drought frequency has increased from once per decade to once every three years, and that human-caused climate change has intensified these trends.
Return to Top	

HEADLINE	**01/04 NFL player's cardiac arrest on football field**
SOURCE	**https://www.seattletimes.com/nation-world/covid-19-vaccines-almost-certainly-didnt-cause-damar-hamlins-cardiac-arrest-heres-what-may-have/**
GIST	Damar Hamlin, the 24-year-old safety with the Buffalo Bills, is not your usual victim of a heart attack. Yet Hamlin on Monday night collapsed roughly nine minutes into the first quarter of a nationally televised football game against the Cincinnati Bengals. Medical personnel on the turf at Paycor Stadium restarted his quivering heart, and he was admitted to University of Cincinnati Medical Center, where he remained in critical condition Tuesday.

Heart disease is the leading cause of death in the United States, killing nearly 70,000 each year. An athlete who plays at the top of a sport that requires strength, superb conditioning and a high tolerance for physical punishment is not the typical victim.

That has led cardiologists and football fans alike to ask: Why did Hamlin's heart stop?

They pondered the velocity and impact point of the hit Hamlin had just meted out. They contemplated his recent illnesses, his medications and his COVID-19 vaccinations. A few acknowledged the grim possibility that his heart had been a ticking time bomb since birth.

Those lines of speculation suggest very different explanations for the highly improbable scenario that played out Monday night.

Sudden cardiac arrest can be the result of trauma, a side effect of medication or a repercussion of heart muscle damage incurred by a viral infection. It can be the predictable outcome of a chronic disease or the first indication of a disease written into a patient's genes at conception.

Sometimes more than one of these contributors is present, muddying the picture.

For doctors trying to keep Hamlin alive, diagnostic tests that create three-dimensional pictures of his heart muscle at work, listen to its rhythms and scan his DNA for telltale mutations may provide clues to what happened.

But medical professionals will not be able to diagnose exactly what happened to his heart at the precise instant he slammed into Bengals wide receiver Tee Higgins.

In the absence of definitive findings from Hamlin's cardiac workup, doctors will have to consider a diagnosis that explains roughly 10 to 20 deaths a year in the United States, mostly among young male athletes: commotio cordis.

"Commotio cordis occurs in people with normal hearts," said Dr. Mark S. Link, a cardiologist at University of Texas Southwestern Medical Center who has written about the unusual cause of sudden cardiac arrest.

Studies in animals suggest that if hit in exactly the right place (where the right ventricle receives blood from the right atrium) and in exactly the right instant (a 20-millisecond span when the walls of the heart are gearing up for their next pump), the stricken ventricles will begin to beat fast and erratically.

Typically, such a precise hit can be delivered by a small projectile — a baseball, puck or lacrosse ball moving at more than 40 miles per hour. Whether a running back's shoulder or elbow could do the same is a scenario not yet studied.

If the heart's disorganized rhythm persists for long enough, the organ will lose its ability to pump blood or sustain normal operations. Unless an automatic external defibrillator and/or chest compressions restore order, death will ensue.

It takes "the perfect storm" of circumstances to result in the death of a seemingly healthy young person, Link said.

The fact that it doesn't happen more often suggests to Link that some young men — the victims are almost exclusively boys and young men — may have underlying conditions that predispose them to such devastating injury.

One of those conditions could be myocarditis, an inflammation of the heart most recently linked to mRNA vaccines for COVID-19. About 95% of all players in the National Football League were vaccinated

	against COVID-19 by the end of last season, so odds are high that Hamlin was one of them. In September, the Centers for Disease Control and Prevention told vaccine experts that among more than 123 million people who received COVID-19 shots, it had detected 131 cases of myocarditis. Most of those cases involved adolescent and young adult males, and none of them died. But myocarditis is far more frequently seen in the wake of run-of-the-mill viral infections; indeed, it was a more common complication among young males who caught the coronavirus than it was among those who got the vaccine, the CDC said. Myocarditis often scars the heart and leaves it weakened years after a case of the flu, herpes simplex or even a common cold. The fingerprints of the virus that caused the damage are rarely visible by the time it's detected. Indeed, one case study published in 2021 found the fingerprint of post-viral myocarditis in a 21-year-old professional rugby player who died on the playing field after he was tackled with a direct blow to the chest. The scarring was revealed in an autopsy, but no one could recall when the offending infection had occurred. Even if myocarditis were found to have contributed to Hamlin's injury, it would more likely stem from "plain, old viral myocarditis" than from a vaccine reaction, Link said, especially since the vast majority of cases related to COVID-19 shots occur within a week of vaccination. "Is it absolutely ruled out?" he said. "No, but it's unlikely."
Return to Top	

HEADLINE	**01/04 Expected AFM surge in kids didn't happen**
SOURCE	**https://abcnews.go.com/US/expected-surge-virus-paralyze-kids-happen-baffling-experts/story?id=96185422**
GIST	*In September, MedPage Today reported on an increase of enterovirus D68 (EV-D68) cases among U.S. children, which has been linked to a rare neurological condition that can cause polio-like paralysis in children. In this report, we follow up on what has happened since those initial reports.* The Centers for Disease Control and Prevention sounded the alarm on EV-D68 with a Health Alert Network Advisory in September announcing that cases were on the rise. Later that month, the agency reported surveillance data showing that rhinovirus, enterovirus, or both were detected in 26.4% of children and adolescents with acute respiratory illness seeking emergency care or requiring hospitalization. Of these, 260 (17.4%) tested positive for EV-D68, and that rate climbed to 56% by mid-August. Of gravest concern was the threat of potential acute flaccid myelitis (AFM), a rare condition associated with EV-D68 that affects the central nervous system predominantly in children, causing muscles and reflexes to become weak and potentially leading to paralysis. Previous outbreaks of AFM had spiked in even-numbered years (2014, 2016, and 2018). However, as of December 1, 2022, the CDC reported that AFM had not surged as expected. "AFM cases have remained low in 2022, despite an uptick in enterovirus D68 circulation and infections," said Dr. Janell Routh, who leads the AFM and domestic polio team for the CDC's Division of Viral Diseases. "This is the first year such a large disconnect between EV-D68 and AFM has been observed since the association was noted in 2014," she said in an email correspondence with MedPage Today. The 30 cases of AFM confirmed at CDC so far this year is similar to numbers in other non-outbreak years, Routh pointed out.

"Given enteroviruses tend to circulate in the late summer and early fall, we expect we will not see an increase in AFM so late in the year," Routh added. "However, EV-D68 circulation was noted in the winter months of 2021-2022, so CDC remains on alert."

As to why the biennial pattern didn't hold up, "no one knows the answer to this right now," Routh told MedPage Today. "In general, it could be the changes in the virus, host factors, or other co-factors that changed this year to alter the course of AFM," she suggested.

Dr. Amy Moore, of Ohio State Wexner Medical Center in Columbus, who works with patients with AFM agreed that the dip is baffling. "Although we have seen more patients affected than in 2021 and 2022, these are not the numbers that we thought we would see given that children are back in school and masks are not mandatory."

Historical patterns for AFM certainly warranted the warning. AFM has been tracked by the CDC since 2014, when 120 cases were reported in 34 states between August and December. In the following year, there were 22 cases reported, then the number rose again in 2016 to 153 cases.

In 2017, it was down again, with 38 cases; then cases increased in 2018 to 238.

The expectation of a surge had also been high in 2020. In August of that year, the CDC called a press conference warning of an expected outbreak of life-threatening acute flaccid myelitis. In particular, the CDC was concerned that cases would be confused with COVID-19.

"AFM can progress quickly and patients can become paralyzed over the course of hours or days and require a ventilator to help them breathe," Dr. Robert Redfield, CDC director at the time, warned during the briefing. "Some patients will be permanently disabled...The virus most commonly causing this condition, enterovirus D68, tends to come in 2-year cycles. This means it will be circulating at the same time as flu and other infectious diseases, including COVID-19, and could be another outbreak for clinicians, parents, and children to deal with."

However, CDC's 2020 surveillance reported 33 AFM cases for 2020 -- lower than anticipated.

"The low numbers were due to the use of masking and the lack of 'in person' activities due to COVID," Moore told MedPage Today. "This trend was also seen with RSV [respiratory syncytial virus] and flu."

It is now unknown whether the biennial pattern is predictive.

From 2014 through December 1, 2022, the CDC has reported a total of 709 cases of AFM.

Cases of this rare but very serious neurological condition have coincided with respiratory illness caused by EV-D68, the antibodies for which are found in mucous and spinal fluid of some patients with AFM.

Researchers recently reopened the case of a boy who died with AFM-suspected illness in 2008 and found EV-D68 RNA in the anterior horn neurons of his spinal cord. They reported the findings earlier this year in The New England Journal of Medicine, noting that "these findings support the view that EV-D68 infection is a cause of AFM. The pathogenesis of AFM may involve a combination of the direct effects of viral infection of spinal cord motor neurons and damage resulting from local inflammation."

Research is ongoing to better understand the causes and treatment of the condition.

"Right now, CDC is finishing data collection on the confirmed cases and will look at how they compare to cases from previous years," Routh told MedPage Today. "Our partners will be looking at how the virus interacts with their animal models of AFM. We continue to work collaboratively across other agencies and academic centers nationwide to better understand AFM."

Return to Top

Crime, Criminals

Top of page

HEADLINE	01/04 Baltimore shooting: teen killed, 4 hurt
SOURCE	https://www.upi.com/Top_News/US/2023/01/04/baltimore-high-school-students-shot/7671672874647/
GIST	Jan. 4 (UPI) -- A high school student was killed and four other students were injured Wednesday in a shooting outside of a Baltimore shopping center. The five students were shot around 11:18 a.m., in the parking lot near a Popeyes restaurant at the Edmondson Village Shopping Center, according to the Baltimore Police Department. The students attend Edmondson Westside High School which is located across the street from the shopping center. Investigators believe they were at the mall during the school lunch break. The school was placed under lockdown as police investigated. "Today, we learned five students were injured after being shot in a shopping center across the street from Edmondson Westside High School," Baltimore City Public Schools wrote in a tweet. "Sadly, one of the students has passed away." Baltimore Police Commissioner Michael Harrison said investigators believe two shooters opened fire on the group before fleeing behind a building. "What we believe is that two shooters began to open fire at the other individuals who were all together in front of the mall," Harrison said at a news conference. Edmondson Westside High School has canceled classes for Thursday, as investigators continue to search for the suspects. "We are now looking for video," Harrison said. "We are looking for witnesses. We are looking for anything that would tell us how this happened, why this happened and who's responsible for it." The student who died was 16-years-old. The injured were two 17-year-old boys and two 18-year-old men, according to police who said the victims were taken to nearby hospitals. "This did not have to happen," Harrison added. "We're talking about the prevalence of guns. We're talking about the willingness to use them. And now we're talking about individuals who are youthful and young being involved in either being a victim of a shooting or pulling that trigger."
Return to Top	

HEADLINE	01/04 Police: 'Office Space' inspired theft scheme
SOURCE	https://www.nytimes.com/2023/01/04/us/seattle-fraud-office-space.html
GIST	A software engineer siphoned more than $300,000 from his employer by introducing what prosecutors called a "series of malicious software edits" that wired money into his personal account. If the scheme sounds like the plot of "Office Space," that's because the authorities said it was partly inspired by the movie. It appears the engineer, Ermenildo Valdez Castro, 28, of Tacoma, Wash., did not watch the entire movie: All of the evidence in the workplace comedy was destroyed in an office fire. But Mr. Castro detailed the scheme in a document found on his company laptop, according to the Seattle police. Mr. Castro, a former software engineer for the e-commerce site Zulily, edited code to divert shipping fees to a personal account and manipulate product prices, stealing about $260,000 in electronic payments and more than $40,000 in merchandise, the police said. He was charged on Dec. 20 with two counts of theft

and one count of identify theft and is scheduled to be arraigned on Jan. 26 in King County Superior Court in Seattle, where Zulily is based.

According to a police report, a document found on Mr. Castro's work laptop referred to the scheme as "OfficeSpace project." He later told the police that he "named his scheme to steal from Zulily after the movie."

In the 1999 film, office workers retaliate against corporate downsizing and their terrible bosses by introducing a computer virus into their company's banking system to embezzle small sums of money. The characters in the film also lifted their scheme from a movie, "Superman III."

Neither Mr. Castro nor Zulily responded to a request for comment. It was not clear if Mr. Castro had a lawyer.

According to court documents, Mr. Castro stole $110,240 by diverting shipping fees from some customers to an account he controlled on the payment-processing site Stripe. After Zulily began an investigation, Mr. Castro wrote a replacement code that double-charged some customers for shipping and routed an additional $151,645 in fees to his Stripe account, the documents say. Investigators discovered that more than 30,000 transactions totaling around $263,300 were paid into Mr. Castro's Stripe account between February and June 2022 that were linked to nearly 25,000 different customer email addresses.

Mr. Castro also manipulated the prices of merchandise sold on Zulily, including a sofa bed, and then purchased those items "for pennies-on-the-dollar," court records show, paying about $250 for nearly 1,300 items collectively worth more than $41,000.

Mr. Castro began working on Zulily's shopping experience team in 2018 and "had direct involvement in the coding of the customer checkout process," the police report said. In the spring of 2022, Mr. Castro began "editing Zulily's software code in ways that allowed him to steal from the company," according to the report, inserting three types of "malicious code" in the checkout process.

He admitted to the police that he had edited the code, but he said that Zulily knew about it and that "it was part of a testing process," according to the police report. He also admitted to using the associated Stripe account to divert the shipping fees, and told the police that the money was "gone" and had been invested in the stock market, particularly in GameStop.

In May, Zulily's fraud team discovered a pattern of steep price adjustments on several products Mr. Castro ordered and had shipped to his home in Tacoma as well as to a female friend whom Mr. Castro later identified as someone he had met on the dating app Tinder. According to the police report, Mr. Castro admitted having placed the orders but said "he had to test an error by sending a large quantity in one order and that he forgot to cancel the items."

Mr. Castro did not return any of the items that were sent to him, and when the police searched his home, officers found "an exorbitant number of these items," some of which were still in their original packaging with a shipping label attached. He was put on administrative leave on June 3 and was terminated six days later, the police report said.

Mr. Castro turned in his company laptop after he was fired, which is when Zulily's cybersecurity team discovered the document labeled "OfficeSpace project." In it, according to the police report, Mr. Castro wrote that his scheme would "cause production traffic to be routed to Stripe." The document detailed the coding needed to pull off the scheme, including a note that he would need to "fudge exposure metrics."

There were also "a number of entries" that indicated that Mr. Castro was preparing to live "off-grid" in the event he was discovered, according to court documents.

Mr. Castro was arrested on July 21 and was held on $999,999 bail. Jail records show he was released two days later.

Return to Top	

HEADLINE	**01/04 Arrest: fire set at Seattle museum facility**
SOURCE	**https://patch.com/washington/seattle/man-who-set-fire-museum-facility-arrested-seattle-police**
GIST	SEATTLE, WA — A man was arrested Wednesday after setting a fire at a museum facility in Georgetown, according to Seattle police. The incident occurred around 3:45 a.m., when witnesses reported seeing the man trying to set bushes on fire in the 5900 block of Sixth Avenue South outside a building that houses a museum operations and storage facility, police said. Officers found exterior fire damage to the building and arrested the 36-year-old, who was digging in a nearby garbage can, according to police. The man had a lighter and butane torch and was booked into King County Jail for reckless burning, police said.
Return to Top	

HEADLINE	**01/04 CBP South Texas $436M illegal drugs 2022**
SOURCE	**https://www.hstoday.us/subject-matter-areas/border-security/cbp-officers-at-south-texas-ports-of-entry-post-significant-increases-in-cocaine-seized-inadmissibles-encountered-in-fy-2022/**
GIST	U.S. Customs and Border Protection (CBP) officers at eight South Texas ports of entry seized a significant amount of narcotics, unreported currency, weapons and uncovered numerous immigration violations during Fiscal Year 2022, most notably a 177 percent increase in inadmissibles encountered and a 19 percent increase in cocaine seized. Fiscal Year 2022 began October 1, 2021 and ended Sept. 30, 2022. “As nonessential traffic resumed early in Fiscal Year 2022, overall workload volumes returned to normal but CBP officers continued to experience the ongoing trend of hard narcotics, particularly cocaine and significant gains in encounters of individuals without valid entry documents,” said (Acting) Director, Field Operations Eugene Crawford, Laredo Field Office. “The hard narcotics volume underscores the seriousness of the drug threat we face and hemispheric economic and security challenges also tend to drive the migration volumes.” During FY 2022, CBP officers at the eight ports of entry extending from Brownsville to Del Rio that comprise the Laredo Field Office seized 47,755 pounds of narcotics that would have commanded a combined estimated street value of $436 million. Specifically, they seized 6,578 pounds of marijuana; 10,243 pounds of cocaine, up 19 percent from FY 21; nearly 30,476 pounds of methamphetamine; 176 pounds of heroin, nearly 282 pounds of fentanyl, $5.8 million in unreported currency, 320 weapons and 78,487 rounds of ammunition. CBP officers at Laredo Field Office ports of entry in FY 2022 also determined that more than 57,732 non-U.S. citizens were inadmissible to the U.S. due to violations of immigration law, up 177 percent over FY 21. CBP agriculture specialists intercepted 99,264 items of quarantine animal and plant material and 5,015 pests.
Return to Top	

HEADLINE	**01/04 France: $24M illegal drugs N. Arabian Sea**
SOURCE	**https://www.hstoday.us/subject-matter-areas/maritime-security/french-warship-seizes-24m-in-illegal-drugs-in-north-arabian-sea/**
GIST	A French warship seized illegal drugs worth a total estimated U.S. street value of $24 million from a fishing vessel transiting international waters in the North Arabian Sea, Dec. 27. French Marine Nationale frigate FS Guépratte (F714) was patrolling regional waters in support of Combined Task Force (CTF) 150 when it seized 3,492 kilograms of hashish and 472 kilograms of heroin

	from the fishing vessel. Led by the Royal Saudi Navy, CTF 150 is one of four task forces organized under the Combined Maritime Forces (CMF), the largest international naval partnership in the world consisting of 34 member-nations. CMF has seized nearly $1 billion worth of illicit narcotics since 2021 while patrolling international waters in the Middle East. Guépratte previously seized 271 kilograms of heroin from another fishing vessel while patrolling the Gulf of Oman in February 2022.
Return to Top	

HEADLINE	**01/05 Tech breakthrough nabs serial child abuser**
SOURCE	**https://www.infosecurity-magazine.com/news/cops-catch-serial-child-abuser/**
GIST	A Pembrokeshire man has been jailed for life for a series of appalling sexual offenses against young children, after investigators used new technology to unmask him. Global law enforcers had been trying to ascertain the identity of 50-year-old Martyn Armstrong for years after abuse material was posted to dark web pedophile site The Love Zone back in 2010. The challenge was that the perpetrator had managed to distort his face in the images to avoid identification, according to the UK's National Crime Agency (NCA). Although Italian investigators linked the name "Martyn" to the perp back in 2017, and French colleagues later identified a beach on the Welsh coast of Pembrokeshire as a possible crime scene, the case remained unsolved until last year. That's when the NCA used innovative new technology to unscramble the image distortion technique Armstrong had used to disguise his identity. Investigators then apparently deployed more traditional policing techniques to search for a "Martyn" with links to that part of the Welsh coast – matching an image from his social media profile with the abuse material. Following Armstrong's arrest on July 30 2022, officers found and forensically matched one of the two cameras he had used to take the images in 2010. They also found the original images on a laptop and, in the process of their investigation, identified two previously unknown child victims, the NCA said. Armstrong pleaded guilty to multiple sex offenses against children under 13 and was yesterday sentenced at Cardiff Crown Court to life with no minimum term. "It is over 17 years since Armstrong began to abuse these young children. I don't believe he thought he would ever be caught and that the distortion techniques he used would protect him," said NCA operations manager, Martin Ludlow. "However, our commitment to identifying him was unwavering and ultimately, NCA officers developed a completely new program which led to his unmasking. Investigators did a remarkable job in piecing together limited information to finally reveal that Armstrong was the person in these images."
Return to Top	

HEADLINE	**01/04 Virginia shooting: 1 dead, 4 teens injured**
SOURCE	**https://www.washingtonpost.com/dc-md-va/2023/01/04/dumfries-shooting-va/**
GIST	A 20-year-old D.C. man has been charged with murder in a shooting that left a 3-year-old girl dead and four teens critically injured at a home in Prince William County, Va., on Wednesday morning, authorities said.

	Kenyatta Lee Oglesby is being held without bond in Prince William County and also charged with aggravated malicious wounding and using a firearm in commission of a felony, county police said. The four surviving victims are a 17-year-old girl, a 16-year-old girl, a 14-year-old girl and a 14-year-old boy. Four of the victims, including the 3-year-old who was killed, are siblings who lived at the residence, according to police. A 13-year-old boy, also a sibling, was in another area of the home and uninjured, police said. They said the 14-year-old boy who was shot was not a sibling but lived at the home. The shooting occurred at a residence in the 17900 block of Milroy Drive in Dumfries, police said. Police responded to the home at about 10:51 a.m. "after someone called the Public Safety Communications Center reporting they had been shot," police said in a news release Wednesday evening. They said they also received other calls of a shooting in the area. Police said a Dumfries police officer was first to arrive at the scene and found one of the victims, the 17-year-old girl, outside in front of the home. Prince William County officers then arrived and checked the inside of the home, where they found four more victims in the basement and provided first aid, police said. The 3-year-old girl was pronounced dead at the scene, according to police. The four other victims were taken to area hospitals with "serious, life-threatening injuries," police said. Police began searching for a person of interest, now identified as Oglesby, and found him along Richmond Highway at a nearby business, police said. They detained him "without incident" and he "became uncooperative with investigators as to what led up to the shooting," police said. According to a preliminary investigation, Oglesby was in a relationship with one of the victims, the 17-year-old girl, and had been staying at the Dumfries home, police said. Oglesby shot her in front of the home, according to police. The four other victims were found inside the home, police said. They said the shootings followed some type of altercation but did not immediately offer details. Police said they recovered two firearms, and ballistics testing will be done to confirm whether the guns were used in the shooting.
Return to Top	

HEADLINE	**01/04 Reward: $500,000 D.C. pipe bombs case**
SOURCE	**https://www.washingtontimes.com/news/2023/jan/4/fbi-increases-reward-info-dc-pipe-bomb-case-500k/**
GIST	The FBI said Wednesday it will offer up to $500,000 to anyone with information leading to the arrest of the person who placed pipe bombs near Republican and Democratic party offices in Washington on the night before the Capitol protest in January 2021. The Washington Field Office said it's trying to pry loose new information two years into the investigation. Previously, the FBI offered $100,000 for valuable data. "With the significantly increased reward, we urge those who may have previously hesitated to contact us — or who may not have realized they had important information — to review the information on our website and come forward with anything relevant," said David Sundberg, assistant director in charge of the FBI Washington Field Office. "Despite the unprecedented volume of data review involved in this case, the FBI and our partners continue to work relentlessly to bring the perpetrator of these dangerous attempted attacks to justice." A suspect wearing a mask, hooded sweatshirt, pants and sneakers was captured by surveillance photos before placing the pipe bombs near the Republican National Committee site on First Street and the Democratic National Committee building on South Capitol Street between 7:30 p.m. and 8:30 p.m. on Jan. 5, 2021. The devices did not detonate, though authorities described them as "viable" bombs that could have harmed

	bystanders. Also, the suspect may still pose a danger "to the public or themselves," the FBI said. The incident was a side plot to the chaos around the Jan. 6 protest by citizens angry over what they perceived as a stolen 2020 presidential election. Many breached the Capitol while Congress was trying to certify Electoral College votes and declare Joe Biden the winner. The FBI said it hopes the increased reward will spur people to look at its "Seeking Information" web page to scrutinize the suspect and circumstances around the case. "We note that many of the components used to build the pipe bombs were widely available for purchase in-store and online. Some of the components used to construct these devices include 1x8-inch threaded galvanized pipes, end caps, kitchen timers, wires, metal clips and homemade black powder," the reward page says. "While additional details cannot be released in order to maintain the integrity of the investigation, the FBI strongly encourages the public to come forward with any relevant information."
Return to Top	

HEADLINE	**01/04 Fraudsters stole, spent pandemic money**
SOURCE	**https://www.washingtontimes.com/news/2023/jan/4/maseratis-and-manicures-how-fraudsters-spent-your-/**
GIST	Valesky Barosy was an up-and-coming entrepreneur, having immigrated from Haiti and quickly making a name for himself in southern Florida as a million-dollar deal-maker. When the pandemic hit, he saw a ticket to even faster wealth by helping others steal from COVID-19 business loan programs. He took up to 30% as his cut that prosecutors said he spent on flashy clothes, fancy watches and a fast car — a Lamborghini Huracan Evo. Barosy, convicted at trial last month for the scam, is far from the only one. For thousands of unscrupulous people, the government's pandemic assistance programs were the equivalent of winning scratch-off lottery tickets. Indeed, that was how Ganell Tubbs, who made off with nearly $2 million in bogus pandemic loans, described her newfound wealth. She sent $150,000 to a relative after saying she had "won the lottery." Upon getting the money, Tubbs treated herself to a two-day online shopping spree at Apple, Michael Kors, North Face and Nike. Jason Carl Pears bought a piano, furniture and luxury goods from Gucci and Louis Vuitton. He also bought two homes, traveled and had plastic surgery. Shaneesha White, who stole nearly $50,000 in unemployment benefits, also used the money to pay for plastic surgery and to buy drugs. Luxury car dealers seem to have been particular favorites for fraudsters, with Maseratis, Mercedes, Teslas and even a Rolls Royce or two zooming off the lots. Rolex watches, exotic trips, plastic surgery and real estate were also popular big-ticket items bought with COVID-19 relief money. Plenty of others, though, said they put their money toward personal expenses. Some made tuition payments; others paid off credit card balances. Jason Scott Carter, a former police officer in Coral Springs, Florida, used $21,788 in bogus pandemic payments to trick out his 1969 Ford Mustang. Marie Springer, who studies white-collar crime as an adjunct associate professor at the John Jay College of Criminal Justice in New York, said some cases bear similarities to white-collar crime, but the chief defining feature of pandemic fraud is that it was a crime of opportunity: The government made money readily available, and people took it. "They do it because they can, because they're greedy and they want it and they somehow feel they're

smart enough to get away with it," she said.

Ms. Springer examined dozens of cases and said the average fraud was $1.9 million, though that amount was skewed by several cases involving much more.

She figured that a majority of fraudsters came in below $1 million.

Ms. Springer found a striking number of women involved. Of the cases she looked at, 23% of the people involved were women. For most white-collar crime, the rate hovers around 10% to 15%, she said.

Some fraudsters claimed altruistic motives.

Oumar Sissoko, an immigrant from Senegal, said he just wanted to build a business with the $7.25 million he received. He didn't realize that the government was paying only for businesses already up and running, he told a judge through his attorney.

"Had he wanted to, he could've brought multiple houses during this time and easily spent the loan money. But he didn't because he intended to do what he wrote on the loan application: build a business," the lawyer said.

Prosecutors said that is tough to square with what Sissoko did spend.

Within days of getting the $7.25 million, Sissoko bought a $100,000 Mercedes. Investigators also connected pandemic money to purchases at Apple, Nordstrom and Birkenstock. All told, he spent $370,000 in the first week.

The only thing that headed off more spending was that his bank realized it had made a mistake and froze the rest of the funds, prosecutors said.

Michael Kornaker began serving supervised release on June 15, 2020, after a 28-month sentence for fraud. That same day, he filed a bogus pandemic loan application using a defunct towing company and his father's identity to hide his felony convictions, which should have blocked him from getting a loan.

His niece ratted him out.

Korner's attorney said his fraud had altruistic motives: He wanted to get the towing company up and running, and he figured his father would want to help him even though he never sought permission to use his identity.

"It was fueled by a harmful desperation to fast forward reintegration in the community and to reestablish a past life," the lawyer said.

Other fraud suspects were blunter about their intentions.

Jeannine R. Buford, accused of helping steal $291,000 in bogus loans, sent a text to a co-conspirator saying there was easy money to be made and she felt it was time she was one of those making it, prosecutors said.

"I'm tired of struggling it's time to put the ski mask on," she texted a friend. "I'm about to get bold as [expletive]! Especially while nobody's paying attention … due to corona."

Porshia L. Thomas, the woman Ms. Buford was texting, has pleaded guilty to her part in the fraud. She spent her money on an Audi S5, living expenses and items from Neiman Marcus, Bath and Body Works and Victoria's Secret.

Brandon Lamar Williams, a would-be rapper from Georgia whom prosecutors described as "a violent,

gun-toting, gang-banging, drug-dealing six-time felon." He was charged with nine counts, including weapons violations.

"Williams simply wanted money, so he committed fraud to obtain it," his attorney told the judge. "There's no underlying reason other than greed."

Luckily for Williams, President Biden's blanket pardon for some marijuana offenses squelched the two drug convictions, and he was left with the pandemic fraud charge. His attorney said that should have earned him a sentence of about 30 months.

Unluckily for Williams, the judge looked at his history of mayhem and slapped him with 60 months in prison.

Jerrod Bellamy, a soldier stationed in Georgia, told the judge his decision to apply for bogus Paycheck Protection Program loans, intended to keep small businesses afloat, was almost a foregone conclusion for someone raised in his circumstances in the Black community.

Indeed, he saw it as just another "hustle." It didn't help that he was going through a divorce and needed money at the same time the government was making cash available.

"PPP loans proved irresistible to those who had grown up engaging in an informal economy within a community that distrusts, holds little respect for, or just tends to be apathetic toward large government agencies in general," Bellamy's attorney told the judge. "There was an opportunity that proved to be very easy to obtain a large amount of cash with victims that for him could easily be rationalized away."

Bellamy has been discharged from the Army. He was slapped with a 22-month prison sentence and ordered to pay back $223,807 in money he stole.

Travis McKenzie, an immigrant from Jamaica, blamed his impoverished upbringing and abandonment by his mother, who fled to the U.S. when he was young. Though he eventually followed her, he still suffered from what his attorney said were "deep-rooted emotional and mental health issues" that led him to drug addiction and later to steal more than half a million dollars in unemployment benefits.

He blew his cash on Louis Vuitton and Prada handbags.

Some fraudsters took thoughtful approaches to their gains and pumped their windfalls into investments.

George Thacker, who had been serving as county executive in Rhea County, Tennessee, paid off his credit card bills with the $650,000 he stole and then siphoned money to his E*Trade account. He also bought Bitcoin, Ether and other cryptocurrencies.

Andrew Aaron Lloyd also looked like he had a serious eye on the future with more than $4 million he bilked from COVID-19 funds.

He bought 25 properties in Oregon and California and transferred $1.8 million to his trading account, where he bought 15,740 shares of Tesla stock. At the time of his sentencing in January 2022, the portfolio was worth more than $18 million.

Not everyone was savvy.

Shaan Diyali pumped $49,000 he received from a bogus small-business loan into a Robinhood stock trading account. He lost it all.

Return to Top

HEADLINE	**01/04 Utah: family of 8 found fatally shot in home**
SOURCE	**https://www.nytimes.com/2023/01/04/us/enoch-utah-shooting-dead.html**

GIST	Eight members of a rural Utah family, including five children, were found fatally shot inside a home in Enoch City on Wednesday, local authorities said. Police officers made the discovery while conducting a "welfare check" at the home, in the agricultural city of about 8,000 people in the southwestern part of the state, nearly 250 miles southwest of Salt Lake City. Local officials did not immediately release any more details about the deceased or the circumstances surrounding the shootings. "At this time, we do not believe there is a threat to the public or that there are any suspects at large," city officials said in a statement on Wednesday. The investigation is continuing, they said. Rob Dotson, the city manager, said that the authorities did not have any information about a motive, and that it would likely take days or longer before they could reach any conclusions about what had taken place inside the home. "We don't know why this happened, and we're not going to guess," Mr. Dotson said in a video statement released to the news media on Wednesday evening. He said that a welfare check is usually conducted when other neighbors raise concerns, or haven't seen fellow residents for an unusual period of time, but would not provide further details on the nature of the call to authorities regarding the family. "This community is feeling remorse, feeling pain," Mr. Dotson said. "There are friends and neighbors and family members who are hurting because of this incident." Neighbors described Enoch City as a tightknit community where homes rarely go up for sale, ensuring that everyone knows one another and making the killings even more shocking. The residential area where police found the victims is often filled with children playing in yards and neighbors who wave hello and volunteer to help one another shovel snow. Richard Jensen, a city councilman, said he had spent the night crying on and off, after learning about the shooting. He pulled himself together to tell his 11-year-old son about what had happened so he didn't have to learn about it in school. "This was a respected community member and church leader, and it is sending shock waves," Mr. Jensen said in an interview. In a statement posted to its website on Wednesday, the Iron County School District in Cedar City, Utah, said that the five children were all students there. The loss was certain to raise "emotions, concerns, and questions for our entire school district, especially our students," school officials said. Aaron Diamond, a resident of Enoch City, said that he knew those killed well, because they attended the same church as him. "They were just a wonderful, wonderful family," he said, adding that the father had worked for an insurance company. "We're all just shocked and heartbroken," Mr. Diamond said. "The people who live here love their neighbors."
Return to Top	

HEADLINE	**01/04 Snohomish Co. standoff ends in arrest**
SOURCE	**https://www.q13fox.com/news/1-person-seriously-injured-in-assault-swat-negotiating-with-suspect-in-snohomish-county**
GIST	SNOHOMISH COUNTY, Wash. - Authorities in Snohomish County have arrested a suspect after he barricaded himself inside a home for several hours.

	According to the Snohomish County Sheriff's Office, deputies were called to the report of an assault with a weapon before 11:00 am. Wednesday to Bothell Everett Highway near 180th St. SE. A woman was taken with life-threatening injuries to the hospital. Deputies said a man barricaded himself inside the home for several hours. "They also used a loud [flash] bang. There were also pepper balls deployed and they tried to negotiate with him through neighboring units in the exterior window," said Courtney O'Keefe, communications director for Snohomish County Sheriff's Office. "I've never seen a police drone fly up and announce to come out with your hands up," said Adam Farr, who lives near the scene. "AK-47s in hand. Scared me back to my apartment, I'll tell you that for sure." The man was arrested at 2:50 p.m. after surrendering to officials. It appears he has self-inflicted injuries and was taken to the hospital. It's unclear what kind of injuries he has. Deputies said that the standoff was happening at an apartment complex and was not impacting traffic on Bothell Everett Highway.
Return to Top	

HEADLINE	**01/04 Bail fund aided man now murder suspect**
SOURCE	**https://komonews.com/news/local/controversial-bail-fund-once-helped-man-now-suspected-of-seattle-murder-northwest-community-bail-fund-police-jail-repeat-offender#**
GIST	SEATTLE, Wash. — The man in custody for Seattle's first homicide of 2023 has previously been bailed out of jail by a nonprofit with a track record of assisting violent, repeat offenders. On Wednesday a judge found probable cause to hold Allister Baldwin in jail for the grisly murder of Ivette Wallin, who lived at the Canaday House in South Lake Union. Police found a bloody knife and drug paraphernalia at the crime scene, according to court documents, and the victim had "signs of physical trauma and significant bleeding" from her neck and shoulder area. Baldwin and the victim knew each other, and police characterized it as a domestic violence incident. Baldwin was non-responsive and refused to attend the court hearing on Wednesday. "Now there's no question that he will stay in the King County Jail because his defense team did not get the chance to argue that he should be released," said Casey McNerthney with the King County Prosecuting Attorney's Office. Baldwin, 46, was previously arrested in 2020 in a domestic violence incident involving another woman. The Northwest Community Bail Fund posted cash bail to help him go free until the trial began. Charges were later dropped when the victim refused to testify for the prosecution. Baldwin could face first-degree murder charges in the latest case involving Wallin. The Northwest Community Bail Fund is a nonprofit group that helps indigent defendants using donations from the public. However, the fund has been known to assist people accused of violent crimes, some of whom are repeat offenders. In May, police said Kylan Houle broke into a Skyway home and shot the father of four who lived there. Months before the alleged murder, the fund put up bail for Houle's release on two pending felony gun charges. Last June, Michael Sedejo was charged with stabbing a man to death at City Hall Park. A month before the

	deadly crime, Sedejo was in jail and charged with assault and robbery until the Northwest Community Bail Fund paid for his release, pending trial. “We hear this most from victims who come to us to say, 'What happened here? Why is this person out,'" McNerthney said. Nearly 52% of the defendants bailed out by the fund since mid-2020 failed to appear for their court dates, according to the King County Prosecuting Attorney’s Office. That compares to 22% of defendants who failed to show up that didn’t get the fund’s help. Also, among those the bail fund assisted, more than 20% were later charged with a new felony versus 15% of defendants who posted bail without the fund. “The public needs to know why judges are making those orders to hold violent people because we don't want victims' voices to be lost," McNerthney said. KOMO News requested an interview with the Northwest Community Bail fund but received a statement instead: "Decisions about fulfilling a request for bail assistance are made on an individual basis and by team consensus, with a focus on reducing harm. Factors that may influence decisions will vary over time and circumstances, for example, availability of funds and Covid outbreaks in jail. Factors that may play a part in our decisions include but are not limited to ability to afford bail amount, health factors, pregnancy, impending loss of job, housing or shelter bed, race, gender status (and) separation of families."
Return to Top	

HEADLINE	**01/04 Credit union closes 2 Seattle sites: crime**
SOURCE	**https://komonews.com/news/local/seattle-credit-union-to-close-two-branches-over-crime-foot-traffic-washington-georgetown-business-bank-money-homeless-police-february-encampment-small-businesses-drugs#**
GIST	SEATTLE, Wash. — Another prominent Seattle business is closing up shop, citing crime concerns and also declining foot traffic following the pandemic. Seattle Credit Union will close two branches in February, on the heels of Starbucks shuttering several stores for similar reasons. People in Georgetown were not surprised to hear their branch will be closing its doors Feb. 3. One restaurant manager nearby believes a lot of the problems with crime and drug use stem from the large homeless camp behind the credit union at 5th and Michigan. “There’s no way I’d let my kids run around here. I don’t even like staying here late,” Kauai Family Restaurant Manager Randi Buza explained. She said Michigan Street has been riddled with drug needles and trash near her family's longtime restaurant, and she's even seen a tent catch fire at the nearby homeless encampment. “I’m surprised [the credit union has] been open this long with that encampment right there and next to that apartment building where a lot of shady stuff has been going down. It’s an eyesore and it’s scary for them,” she added. The credit union, in a statement, said the decision to close their Georgetown and Rainier branches was years in the making, stemming from a loss of foot traffic and more electronic transactions during the COVID-19 pandemic. It’s also weighed branch safety issues and security costs, according to the statement. “What crime haven’t I noticed around here, from break-ins burglaries, theft?” asked Todd Reed of Seattle. Reed uses the Rainier branch's ATM but said he'd rather see the workers move somewhere safer until

	there's more help for people in the area with mental illness. “Unless they’re addressed or have a place they can go to where they feel safe and are reconditioned into getting back into society, they’re just going to wander around the streets and victimize or be victimized,” Reed stated. Meanwhile, Buza said she believes her neighborhood needs more police, while acknowledging the staffing crisis. “It’s pretty sad. I think the city in the last few years has kind of let the people down, especially small businesses like us. It’s kind of survival of the fittest out here,” she said. The credit union added they can keep serving the community through their other branches and online services. KOMO News reached out to the mayor's office for a response to the loss of more businesses over crime concerns, but has yet to hear back.
Return to Top	

HEADLINE	**01/04 FBI directed cops to pull over suspect**
SOURCE	**https://www.foxnews.com/us/idaho-murders-fbi-directed-indiana-police-pull-over-bryan-kohberger-seeking-video-images-hands**
GIST	MOSCOW, Idaho – A Federal Bureau of Investigation surveillance team tracked Idaho quadruple murder suspect Bryan Kohberger and his father on a cross-country road trip from Washington State to Pennsylvania and asked Indiana police to pull him over, a law enforcement source told Fox News. The law enforcement source told Fox News that the FBI surveillance team was seeking video images of Kohberger as well as his hands. Bryan Kohberger and his father were pulled over twice in Indiana on Dec. 15 while making the cross-country trip. The law enforcement source said that investigators were still building their case on Dec. 15 to make an arrest, but added that genealogy played a major role. Bryan Kohberger is being charged in connection to the fatal Nov. 13 stabbings of University of Idaho students Kaylee Goncalves, Ethan Chapin, Xana Kernodle and Madison Mogen during the early morning hours in Moscow, Idaho. During a traffic stop by the Hancock County Police Department, the Kohbergers discussed an incident near Washington State University where a SWAT team killed an armed man amid a standoff. "Well, we're coming from WSU," Kohberger's father, Michael Kohberger says. "What's WSU?" the deputy says. Both men replied at the same time, and the deputy had a hard time hearing them over the vehicles passing by. "So you're coming from Washington State University, and you're going where?" the deputy asks. "We're going to Pennsylvania," Kohberger's father responded. Kohberger signed an extradition document during a court hearing on Tuesday afternoon and waived his right to challenge the arrest on four counts of first-degree murder.

	"Yes," Kohberger said when Judge Margherita Worthington asked if he wishes to "waive the rights that I have just explained to you and return to the state of Idaho?" Kohberger, a teaching assistant and Ph.D. student at Washington State University's Department of Criminal Justice, was arrested on Dec. 30 by local police and agents from the Federal Bureau of Investigation at his parents' home in Albrightsville. The suspect lives in student housing located in Pullman, Washington, around 10 minutes from where the crime happened.
Return to Top	

HEADLINE	**01/04 Police traffic stop Idaho suspect twice**
SOURCE	**https://www.nytimes.com/2023/01/04/us/idaho-murders-kohberger-suspect.html**
GIST	MOSCOW, Idaho — The man accused of killing four University of Idaho college students received a new license plate for his car five days after the murders, according to records released Wednesday. The licensing documents in Washington State show that the vehicle driven by the suspect, Bryan Kohberger, was a white Hyundai Elantra, the type of vehicle that investigators had been seeking in recent weeks. The police in Moscow had said that a white Hyundai Elantra from between 2011 and 2013 had been seen near the scene of the crimes on the night of the killings in Moscow, Idaho, on Nov. 13. Mr. Kohberger's car was a 2015 model and registered on Nov. 18, according to the licensing document. A vehicle history report shows the car had previously been registered in Pennsylvania, where Mr. Kohberger is from. Mr. Kohberger, 28, had moved to Pullman, Wash., in recent months and began studying criminology in a Ph.D. program at Washington State University in August. He has said through a lawyer that he expects to be exonerated in the case. Mr. Kohberger's new lawyer did not immediately respond to a request for comment on the license plate records. On Wednesday, the police in Indiana released new body camera footage showing that, two weeks before Mr. Kohberger was arrested, the police there had pulled him over twice in a 10-minute stretch for tailgating. The traffic stops, on Dec. 15, came as Mr. Kohberger was driving across the country with his father for winter break in the same car for which he had obtained the new license plate. During both stops, the suspect's father mentioned a fatal police standoff that took place that morning near Washington State University, where his son was a student, and told the officer that he and his son had been discussing the "horrifying" incident. The police shooting that they were discussing does not appear to have any connection to the four fatal stabbings that occurred about a month earlier in Idaho, just across the border from the W.S.U. campus. Mr. Kohberger is now charged with four counts of murder in the stabbings. Mr. Kohberger was the driver of the car during both stops, and the new footage is the most that the public has seen of him since he became the subject of intense scrutiny after his arrest. On Wednesday, Mr. Kohberger was flown by the police from Pennsylvania, where he was visiting his parents after the road trip, to Idaho, where he stands accused of stabbing four students to death overnight in their home on Nov. 13. The Pennsylvania State Police plane touched down at the Pullman-Moscow Regional Airport shortly before 6:30 p.m., and Mr. Kohberger was booked into the Latah County Jail in Moscow. Mr. Kohberger's father, Michael Kohberger, visited him in December, and they drove across the country from the W.S.U. campus in Pullman, Wash., to their home in eastern Pennsylvania. During that trip, they were pulled over twice on Dec. 15 for tailgating; in both traffic stops, the officers let the men off with a

warning.

There is no indication that the police in Indiana had any idea that Mr. Kohberger would be arrested for the murders, or that they were aware of the police in Moscow, Idaho, saying that a white Hyundai Elantra had been seen near the crime scene on the night of the murders.

During the first stop, at about 10:42 a.m., a deputy with the Hancock County Sheriff's Department pulled Mr. Kohberger and his father over along Interstate 70, just east of Indianapolis. The body camera footage released on Wednesday captured the deputy asking where the two were headed. In response, Mr. Kohberger's father said that they were coming from Washington and had been talking about the police standoff that was unfolding near the Washington State campus that day.

Mr. Kohberger's father told the officer that there had been a "mass shooting." He was corrected by his son, who said, "We don't know if it was a mass shooting," and referred to a SWAT team being called for the standoff. "It's horrifying," Mr. Kohberger's father said in the video. That incident involved a man who the police later said had barricaded himself in an apartment and threatened to kill his roommates before a police officer shot him to death.

At another point in the video, the father said, "We're slightly punchy because we've been driving for hours."

After about three minutes, the deputy said, "Do me a favor and don't follow too close, OK?" and then returned Mr. Kohberger's driver's license and let them go.

Just five minutes later, Mr. Kohberger and his father were pulled over again, this time by an Indiana state trooper who also said that they were tailgating. The audio from the trooper's body camera is obscured by traffic noise, but Mr. Kohberger and his father could be heard telling the officer that they were just stopped minutes earlier. Again, the father brought up the incident that morning at Washington State. The trooper wished them a safe trip and let them go with a warning.

It was two weeks later, on Dec. 30, that the police in Pennsylvania carried out a predawn raid of Mr. Kohberger's parents' home, arresting Mr. Kohberger on suspicion of carrying out the Idaho killings. They also searched his car and executed a warrant to obtain his DNA, officials said. Mr. Kohberger has said through a public defender that he looks forward to being exonerated.

Mr. Kohberger had just completed his first semester at Washington State, which is about a 15-minute drive from the crime scene in Moscow. Classmates said he had shown an interest in the psychology of criminals as well as in forensics.

The murders of the four University of Idaho student victims — Madison Mogen, 21; Kaylee Goncalves, 21; Xana Kernodle, 20; and Ethan Chapin, 20 — and the arrest of Mr. Kohberger have rattled the neighboring college towns of Moscow and Pullman.

The stabbing took place in the early morning hours at a home along a dead-end street a five-minute walk from campus. The police have said that the victims were most likely asleep when they were attacked, and two more roommates were in the home but apparently slept through the killings.

Friends and relatives of the victims are searching for any connection between the victims and Mr. Kohberger, but so far none has been disclosed.

The police have said that the surviving roommates realized something was wrong only late in the morning and believed that one of their roommates had passed out. They called friends to the home and then someone called 911, after which police officers discovered the grisly scene.

Return to Top

HEADLINE	**01/05 Genetic genealogy nabs Idaho suspect**

SOURCE	**https://www.foxbusiness.com/lifestyle/idaho-murder-suspect-nabbed-genetic-genealogy-sites-work-law-enforcement**
GIST	DNA databases have been highlighted amid reports the arrest of the Moscow, Idaho quadruple homicide suspect was aided by genetic genealogy. Moscow police announced last week a Washington State University graduate student, Bryan Kohberger, had been arrested in connection to the Nov. 13 murders of four University of Idaho students, charging him murder and felony burglary. Victims Kaylee Goncalves, Madison Mogen, Ethan Chapin and Xana Kernodle were found fatally stabbed in the girls' rental home. The alleged perpetrator's arrest came after authorities matched DNA from the crime scene to a sample on a genealogy testing website that was submitted by a family member of his, a law enforcement source told Fox News. How, if at all, DNA databases work with law enforcement in criminal cases varies. GEDmatch shares information with law enforcement in certain instances. It changed its policy in 2019 so users have to opt-in for their information to be accessible to police. When users select the "Public Opt-in" option, their DNA will be "compared with kits submitted by law enforcement to identify perpetrators of violent crimes," according to GEDmatch's website. Kits do not get run against ones uploaded by authorities to find violent crime perpetrators if users choose the "Public Opt-out" option. Selecting "private" prevents all matching. "Law enforcement is not allowed to use GEDmatch per our Terms of Service," Swathi Kumar, a spokesperson for parent company Verogen, said to FOX Business. "They are required to use GEDmatch PRO, which is a purpose built digital portal for forensic use." The upload process for GEDmatch PRO, Kumar said, allows investigators to "compare DNA kits from unidentified human remains against the entire GEDmatch database" and "compare DNA kits from violent crimes such as sexual assault and homicides against a limited set of DNA kits in the GEDmatch database that have actively elected to opt-in for such comparisons." Its algorithms "only surface metadata associated with the DNA kits such as the name (alias), email ID and the genetic distance between the compared kits to investigations," Kumar said. Meanwhile, 23andMe told FOX Business it does "not share customer information with law enforcement." On its privacy webpage, it says it "will not release any individual-level personal information to law enforcement without your explicit consent unless required by law." 23andMe "closely scrutinizes all law enforcement and regulatory requests," only complying with ones the company "determine[s] are legally valid and legally require our response after exhausting other options," it said in 2021. According to its transparency report, 23andMe has received 11 government requests for data about 15 customers or accounts from 2015 to mid-October. It did not provide the data in those instances. Genealogy company Ancestry.com has similar policies regarding sharing genetic information with police. Its privacy page states the company does not "voluntarily provide data of any kind to governmental or judicial bodies or to law enforcement agencies" unless a "valid legal process" like a subpoena or warrant requires it. The company does not let police use it to "investigate crimes or to identify human remains." Ancestry has received a few DNA-related requests over the years, though it does not appear to have provided such information apart from one 2014 instance involving a sample that had "previously been made public for which the police had a match," according to its transparency reports. It has provided non-genetic information for investigations into crimes like credit card misuse and fraud in a handful of

	instances. A spokesperson confirmed the company's policy to FOX Business, adding Ancestry has not had any involvement with the Moscow murders case. FamilyTreeDNA, owned by Gene by Gene, provides law enforcement with access to DNA matches from users who have opted to participate in its Investigative Genetic Genealogy Matching (IGGM) on a case-by-case basis for certain crimes. "Gene by Gene has a thorough vetting process for law enforcement use of FamilyTreeDNA's database," FamilyTreeDNA told FOX Business. "All cases are reviewed and accepted based on strict guidelines before they are approved to be uploaded." Users are only viewable to law enforcement accounts if they have "opted into matching," not declined participating in IGGM, have the "same matching levels selected" as the LE account and are genetic relatives to the DNA file authorities submitted, per FamilyTreeDNA's website. "The actual DNA profiles of customers are not shared; the only information available is a list of matches, their predicted relationship, the total amount of DNA shared and the longest block of shared DNA," its statement continued. Customers are "completely excluded from law enforcement match lists" if they have opted out of IGGM, the company added. FamilyTreeDNA said in a report it has received two law enforcement requests "not applicable" to its terms of service. It has "not received any valid subpoenas for FamilyTreeDNA user information" since the transparency report, last updated in March, was first published in 2019, it said. The companies all say that unless legally barred from doing so, they will notify customers if a valid legal process compels them to provide information to authorities. The FBI declined to comment on what commercial DNA databases it works with.
Return to Top	

HEADLINE	**01/04 'Varsity Blues' mastermind jailed 42mo.**
SOURCE	**https://abcnews.go.com/US/mastermind-varsity-blues-college-cheating-scandal-sentenced/story?id=96080462**
GIST	BOSTON -- William "Rick" Singer, the ringleader in a college admissions cheating scandal that spanned the country, was sentenced to 42 months in prison by a federal judge on Wednesday. Singer will then be on supervised release for three more years. He will turn himself over to authorities on Feb. 27. The former college admissions consultant pleaded guilty in March 2019 to helping parents of dozens of well-to-do high school students cheat their way into elite universities. His sentence comes nearly four years after his plea, as he helped prosecutors convict his former clients, including high-powered executives, fashion moguls and Hollywood actors Felicity Huffman and Lori Loughlin. Singer, 62, pleaded guilty to charges of racketeering conspiracy, money laundering conspiracy, conspiracy to defraud the United States and obstruction of justice. Prosecutors had asked for a sentence of six years in prison -- much more than the six-month maximum Singer's lawyers requested.

Prosecutors called it the "most massive fraud" ever perpetrated in the U.S. education system.

"Without this defendant, without Rick Singer coming up with a scheme, masterminding the scheme, orchestrating the scheme it never would have happened," the prosecutor said.

Singer's lawyer Candice Fields said Wednesday in a statement: "It was a sobering day in court but Rick is resilient and committed to a future dedicated to the underserved. He hopes to continue making amends for mistakes of the past."

His sentence all but marks the end of "Operation Varsity Blues," the moniker for the FBI's investigation that uncovered a cheating ring of approximately 50 defendants.

Among those prosecuted were parents who paid Singer more than $6 million, Ivy League coaches who opened sham spots on their rosters for Singer's clients in exchange for bribes and test administrators who were paid to fudge applicants' entrance exam scores.

Prosecutors said Singer was the mastermind of the decadeslong scheme, which has since become the subject of at least four books, a Lifetime movie and a Netflix documentary.

"He is the architect, he is the face of this fraud," the prosecutor said.

Before the sentencing, Singer read a letter apologizing to students whose parents paid him to bribe their kids' way into school, to some of the institutions, and to his family and friends.

"Those students were intelligent and deserving of more integrity than I showed them," he read aloud in court.

"I can see the difference between how I was and how I am now and always want to be," he said. "All I want to do is live a life that is deeper and more enriched by devoting myself to making a difference in other people's lives," he continued.

"Despite my passion to help others, I have lost my ethical values and I have so much regret. To be frank, I am ashamed of myself," he also said.

Singer sat slumped in his chair between his two attorneys throughout the hearing, and did not react to the sentence.

He had convinced wealthy clients to pay him bribes in order to give their children a leg up at schools such as Yale, Georgetown and the University of Southern California, prosecutors said. Singer then funneled the money through his charity he said would support disadvantaged youth, allowing his co-conspirators to write off their dues as tax deductions.

Singer was "exceptionally valuable" following his plea deal, according to prosecutors' sentencing memorandum. He agreed to have his phone tapped to help indict his former clients and accomplices, allowing the government to secure the convictions.

Still, his cooperation was laden with missteps, prosecutors wrote. He met in person with at least six of his former clients to warn them about the investigation and was subsequently convicted of obstructing justice.

"He was the architect and mastermind of a criminal enterprise that massively corrupted the integrity of the college admissions process," prosecutors wrote in the memorandum.

"Without Singer, the scheme never would have happened," they added.

In his own memorandum, Singer wrote that he had forfeited his assets, including a sprawling mansion in

	Orange County, California, which he exchanged for a modest home in a Florida trailer park. "I have been reflecting on my very poor judgment and criminal activities that increasingly had become my way of life," he wrote. "I have woken up every day feeling shame, remorse and regret."
Return to Top	

HEADLINE	**01/04 CBP: $9.1M cocaine Puerto Rico ferry boat**
SOURCE	**https://abcnews.go.com/US/91-million-cocaine-seized-puerto-rico-ferry-border/story?id=96190274**
GIST	U.S. customs officers seized 877 pounds of cocaine concealed on board a Caribbean ferry boat in a single bust over the holidays, according to Customs and Border Protection. The value of the seized cocaine was estimated at $9.1 million. “Our experienced CBP officers remain vigilant, utilizing their training and available tools to stop dangerous drugs from entering the country,” the port of entry director for Puerto Rico, Roberto Vaquero, said in a statement on Tuesday. On Dec. 26, officers noticed a hidden compartment during a routine cargo inspection of the arriving boat at a dock in San Juan, Puerto Rico, where they discovered 355 tightly wrapped packages that were the size of bricks, CBP said. The contents later tested positive for cocaine. Registered in the Bahamas, the vessel regularly transits through the Caribbean Sea between Puerto Rico and the Dominican Republic, according to authorities. The seizure comes amid a surge of migration across the Caribbean. U.S. officials in south Florida have seen a 400% increase in migrant encounters so far this fiscal year compared to the same period last year, Border Patrol Chief Raul Ortiz said Wednesday. Officials based out of the Miami region have tracked and disrupted 26 human smuggling events involving nearly 600 migrants in the past five days alone, Ortiz said. The transnational criminal organizations that facilitate human smuggling are often the same groups that traffic weapons and drugs, U.S. officials say.
Return to Top	

Information From Online Communities and Unclassified Sources/InFOCUS is a situational awareness report published daily by the Washington State Fusion Center.

If you no longer wish to receive this report, please submit an email to intake@wsfc.wa.gov and enter UNSUBSCRIBE InFOCUS in the Subject line.

use of previously copyrighted materials if the purposes of display include 'criticism, comment, news reporting, teaching, scholarship, and research.' Section 107 establishes four criteria for determining whether the use of a work in any particular case qualifies as a 'fair use'. A work used does not necessarily have to satisfy all four criteria to qualify as an instance of 'fair use'. Rather, 'fair use' is determined by the overall extent to which the cited work does or does not substantially satisfy the criteria in their totality. If you wish to use copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner. For more information go to: <http://www.law.cornell.edu/uscode/17/107.shtml>

Source: http://www.law.cornell.edu/uscode/17/107.shtml

Return to Top